#2 KWS 5-14-01

Atty. Dkt. No. 072982/0214

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Satoshi OBANA

Title: SIGNATURE CALCULATION SYSTEM BY USE OF MOBILE AGENT

Appl. No.: Unassigned

Filing Date: 1/17/2001

Examiner: Unassigned

Art Unit: Unassigned

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

- Japan Patent Application No. 2000-009037 filed 1/18/2000.

Respectfully submitted,

Date January 17, 2001

By Thomas G. Bilodeau Reg No 43,438

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

for David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

SATOSHI OBANA
72982/214

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年 １月１８日

出願番号
Application Number: 特願２０００－００９０３７

出願人
Applicant (s): 日本電気株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２０００年１０月１３日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３０８４３８３

【書類名】　特許願

【整理番号】　33509672

【提出日】　平成12年 1月18日

【あて先】　特許庁長官　殿

【国際特許分類】　G09C　1/00

H04L　9/32

【発明の名称】　移動エージェントによる署名計算システムおよびプログラムを記録した記録媒体

【請求項の数】　7

【発明者】

【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内

【氏名】　尾花　賢

【特許出願人】

【識別番号】　000004237

【氏名又は名称】　日本電気株式会社

【代理人】

【識別番号】　100108578

【弁理士】

【氏名又は名称】　髙橋　詔男

【代理人】

【識別番号】　100064908

【弁理士】

【氏名又は名称】　志賀　正武

【選任した代理人】

【識別番号】　100101465

【弁理士】

【氏名又は名称】　青山　正和

【選任した代理人】

【識別番号】　100108453

【弁理士】

【氏名又は名称】　村山　靖彦

【手数料の表示】

【予納台帳番号】　008707

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9709418

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　移動エージェントによる署名計算システムおよびプログラムを記録した記録媒体

【特許請求の範囲】

【請求項１】　移動エージェントがプログラムコードの実行を行うエージェント実行環境と、

乱数を出力する乱数生成手段と、

乱数生成手段から出力される乱数と移動エージェントの所有者の秘密鍵とを入力として、移動先のホストで移動エージェントが署名を計算するために必要な補助データを生成する部分署名補助データ生成手段と、

計算されたデータの秘匿および署名の付与を行う公開鍵暗号計算手段とを備えたベースホストを出発点として前記移動エージェントが移動を開始し、

移動エージェントがプログラムコードの実行を行うエージェント実行環境と、

署名対象データと移動エージェントが保有しているデータと移動先ホストの秘密鍵とを入力として移動エージェントが署名を計算するために必要なデータである部分署名を計算する部分署名計算手段と、

移動先ホストによって計算された一つまたは複数の部分署名を入力として前記署名対象データに対する移動エージェントの所有者の秘密鍵を用いて計算を行ったディジタル署名を出力する部分署名署名化手段と、

計算されたデータの秘匿および移動先ホストの署名付与を行う公開鍵暗号計算手段とをそれぞれ備えた一つまたは複数の移動先ホストを前記移動エージェントが移動することによって、移動エージェントが移動先のホストで任意の署名対象データに対する移動エージェントの所有者の秘密鍵を用いたディジタル署名を計算することを特徴とする移動エージェントによる署名計算システム。

【請求項２】　移動エージェントがプログラムコードの実行を行うエージェント実行環境と、

乱数を出力する乱数生成手段と、

乱数生成手段から出力される乱数を入力として、新規秘密鍵・公開鍵のペアと移動先のホストで移動エージェントが署名を計算するために必要な補助データを

生成する部分署名補助データ生成手段と、

計算されたデータの秘匿および署名の付与を行う公開鍵暗号計算手段とを備えたベースホストを出発点として前記移動エージェントが移動を開始し、

移動エージェントがプログラムコードの実行を行うエージェント実行環境と、

署名対象データと移動エージェントが保有しているデータと移動先ホストの秘密鍵とを入力として移動エージェントが署名を計算するために必要なデータである部分署名を計算する部分署名計算手段と、

移動先ホストによって計算された一つまたは複数の部分署名を入力として前記署名対象データに対するベースホストの部分署名補助データ生成手段によって出力された前記新規秘密鍵を用いて計算を行ったディジタル署名を出力する部分署名署名化手段と、

計算されたデータの秘匿および移動先ホストの署名付与を行う公開鍵暗号計算手段とをそれぞれ備えた一つまたは複数の移動先ホストを前記移動エージェントが移動することによって、移動エージェントが移動先のホストで任意の署名対象データに対する前記新規秘密鍵を用いたディジタル署名を計算することを特徴とする移動エージェントによる署名計算システム。

【請求項３】　前記移動ホストにおける部分署名計算手段と部分署名署名化手段と公開鍵暗号計算手段とのうちの何れか一つ以上を移動エージェント側に設けたことを特徴とする請求項１または２記載の移動エージェントによる署名計算システム。

【請求項４】　移動エージェントがプログラムコードの実行を行うエージェント実行処理と、

乱数を出力する乱数生成処理と、

乱数生成処理で生成された乱数と移動エージェントの所有者の秘密鍵とを入力として、移動先のホストで移動エージェントが署名を計算するために必要な補助データを生成する部分署名補助データ生成処理と、

計算されたデータの秘匿および署名の付与を行う公開鍵暗号計算処理とを実行するためのプログラムを記録した記録媒体。

【請求項５】　移動エージェントがプログラムコードの実行を行うエージェ

ント実行処理と、

署名対象データと移動エージェントが保有しているデータと移動先ホストの秘密鍵とを入力として移動エージェントが署名を計算するために必要なデータである部分署名を計算する部分署名計算処理と、

移動先ホストによって計算された一つまたは複数の部分署名を入力として前記署名対象データに対する移動エージェントの所有者の秘密鍵を用いて計算を行ったディジタル署名を出力する部分署名署名化処理と、

計算されたデータの秘匿および移動先ホストの署名付与を行う公開鍵暗号計算処理とを実行するためのプログラムを記録した記録媒体。

【請求項６】　移動エージェントがプログラムコードの実行を行うエージェント実行処理と、

乱数を出力する乱数生成処理と、

乱数生成処理で生成された乱数を入力として、新規秘密鍵・公開鍵のペアと移動先のホストで移動エージェントが署名を計算するために必要な補助データを生成する部分署名補助データ生成処理と、

計算されたデータの秘匿および署名の付与を行う公開鍵暗号計算処理とを実行するためのプログラムを記録した記録媒体。

【請求項７】　移動エージェントがプログラムコードの実行を行うエージェント実行処理と、

署名対象データと移動エージェントが保有しているデータと移動先ホストの秘密鍵とを入力として移動エージェントが署名を計算するために必要なデータである部分署名を計算する部分署名計算処理と、

移動先ホストによって計算された一つまたは複数の部分署名を入力として前記署名対象データに対するベースホストの部分署名補助データ生成処理で生成された前記新規秘密鍵を用いて計算を行ったディジタル署名を出力する部分署名署名化処理と、

計算されたデータの秘匿および移動先ホストの署名付与を行う公開鍵暗号計算処理とを実行するためのプログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ベースホストを出発した移動エージェントが移動先ホストにおいてディジタル署名を計算する場合に用いて好適な移動エージェントによる署名計算システムおよびベースホスト、移動ホストでそれぞれ用いられるプログラムを記録した記録媒体に関するものである。

【０００２】

【従来の技術】

移動エージェントは、移動エージェントの所有者の依頼した目的を達成するために、ネットワーク上に存在する複数のホストを自律的かつ動的に移動し、移動先のホストでプログラム・コードを起動し、処理していく。移動エージェントのセキュリティを保護する方式としては、移動エージェントのプログラム・コードの中に、公開鍵暗号や秘密鍵暗号のアルゴリズムを実装したプログラム・コードを格納して、悪意のある第三者によるデータの解析を困難にする方式や、移動エージェントのプログラム・コードに対して該移動エージェントの所有者の秘密鍵を用いて計算を行ったディジタル署名のデータをエージェントに保有させてネットワークを移動させる事によって、移動エージェントのプログラム・コードや保持するデータの改竄を困難にする方式が提案されている。

【０００３】

移動エージェントのセキュリティ保護に関する従来技術は、例えば特開平１０－２６９１８６号公報や特表平１１－５０６２２２号公報に詳しく述べられている。

【０００４】

【発明が解決しようとする課題】

上記特開平１０－２６９１８６号公報で述べられている技術では、悪意のある第三者がデータの解析や改竄を行う事を防止する事はできるが、移動先のホストに悪意がある場合には、移動先のホストによって移動エージェントの保有しているデータの解析が容易に行えるという問題がある。移動エージェントが移動先のホストでエージェントの所有者のディジタル署名を計算しようとする場合、エー

ジェントは該所有者の秘密鍵をエージェントに保有させる必要があるため、移動先のホストは、移動エージェントの保有するプログラム・コードおよびデータを解析する事により、該ユーザの秘密鍵を容易に知る事が可能であった。

【０００５】

この問題のため従来の技術では、移動エージェントが移動先のホストで該ホストが提示した任意のデータに対してディジタル署名を施す事は不可能であった。

【０００６】

また、特表平１１－５０６２２２号公報に述べられている技術では、署名計算を委託する移動ホスト等の機関が多数ある場合には、効率的の面で問題があった。尚、この公報の技術については、後述によりさらに説明する。

【０００７】

本発明の目的は、単独の移動先のホストでは解析できない形態で移動エージェント所有者の秘密鍵を移動エージェントに保有させる事により、移動先のホストに秘密鍵を知られる事なく、任意の移動先のホストが提示した任意の署名対象データに対する前記移動エージェント所有者のディジタル署名を計算し、前記署名対象データを提示した移動先のホストに渡す事にある。

【０００８】

また、本発明の他の目的は、単独の移動先のホストでは解析できない形態で移動エージェントの所有者にしか生成し得ない情報を移動エージェントに保有させる事により、任意の移動先のホストが提示した任意の署名対象データに対して前記情報を秘密鍵として用いたデジタル署名を計算し、前記署名対象データを提示した移動先のホストに渡す事にある。

【０００９】

【課題を解決するための手段】

上記の目的を達成するために、本発明による第１の移動エージェントによる署名計算システムは、移動エージェント（例えば第１の形態および第１の実施例における移動エージェント１４０、５４０）がプログラムコードの実行を行うエージェント実行環境（同実行環境１０５、５０５）と、乱数を出力する乱数生成手段（同乱数生成部１０１、５０１）と、乱数生成手段から出力される乱数と移動

エージェントの所有者の秘密鍵（同秘密鍵１０３、５０３）とを入力として、移動先のホスト（同移動先ホスト１１０、１２０、１３０、５１０、５２０、５３０）で移動エージェントが署名を計算するために必要な補助データを生成する部分署名補助データ生成手段（同部分署名補助データ生成部１０４、５０４）と、計算されたデータの秘匿および署名の付与を行う公開鍵暗号計算手段（同公開鍵暗号計算部１０２、５０２）とを備えたベースホスト（同ベースホスト１００、５００）を出発点として前記移動エージェントが移動を開始し、移動エージェントがプログラムコードの実行を行うエージェント実行環境（同実行環境１１１、１２１、１３１、５１１、５２１、５３１））と、署名対象データと移動エージェントが保有しているデータと移動先ホストの秘密鍵（同秘密鍵１１５、１２５、１３５、５１５、５２５、５３５）とを入力として移動エージェントが署名を計算するために必要なデータである部分署名を計算する部分署名計算手段（同部分署名計算部１１２、１２２、１３２、５１２、５２２、５３２）と、移動先ホストによって計算された一つまたは複数の部分署名を入力として前記署名対象データに対する移動エージェントの所有者の秘密鍵を用いて計算を行ったディジタル署名を出力する部分署名署名化手段（同部分署名署名化部１１３、１２３、１３３、５１３、５２３、５３３）と、計算されたデータの秘匿および移動先ホストの署名付与を行う公開鍵暗号計算手段（同公開鍵暗号計算部１１４、１２４、１３４、５１４、５２４、５３４）とをそれぞれ備えた一つまたは複数の移動先ホストを前記移動エージェントが移動することによって、移動エージェントが移動先のホストで任意の署名対象データに対する移動エージェントの所有者の秘密鍵を用いたディジタル署名を計算することを特徴とする。

【００１０】

また、本発明による第２の移動エージェントによる署名計算システムは、移動エージェント（例えば第２の形態および第２の実施例における移動エージェント３４０、７４０）がプログラムコードの実行を行うエージェント実行環境（同実行環境３０５、７０５）と、乱数を出力する乱数生成手段（同乱数生成部３０１、７０１）と、乱数生成手段から出力される乱数を入力として、新規秘密鍵・公開鍵のペアと移動先のホストで移動エージェントが署名を計算するために必要な

補助データを生成する部分署名補助データ生成手段（同部分署名補助データ生成部３０４、７０４）と、計算されたデータの秘匿および署名の付与を行う公開鍵暗号計算手段（同公開鍵暗号計算部３０２、７０２）とを備えたベースホスト（同ベースホスト３００、７００）を出発点として前記移動エージェントが移動を開始し、移動エージェントがプログラムコードの実行を行うエージェント実行環境（同実行環境３１１、３２１、３３１、７１１、７２１、７３１））と、署名対象データと移動エージェントが保有しているデータと移動先ホストの秘密鍵（同秘密鍵３１５、３２５、３３５、７１５、７２５、７３５）とを入力として移動エージェントが署名を計算するために必要なデータである部分署名を計算する部分署名計算手段（同部分署名署名化部３１３、３２３、３３３、７１３、７２３、７３３）と、移動先ホストによって計算された一つまたは複数の部分署名を入力として前記署名対象データに対するベースホストの部分署名補助データ生成手段によって出力された前記新規秘密鍵を用いて計算を行ったディジタル署名を出力する部分署名署名化手段（同部分署名署名化部３１３、３２３、３３３、７１３、７２３、７３３）と、計算されたデータの秘匿および移動先ホストの署名付与を行う公開鍵暗号計算手段（同公開鍵暗号計算部３１４、３２４、３３４、７１４、７２４、７３４）とをそれぞれ備えた一つまたは複数の移動先ホストを前記移動エージェントが移動することによって、移動エージェントが移動先のホストで任意の署名対象データに対する前記新規秘密鍵を用いたディジタル署名を計算することを特徴とする。

【００１１】

また、第１、第２の移動エージェントによる署名計算システムにおいて、移動ホストを構成する部分署名計算手段、部分署名署名化手段および公開鍵暗号計算手段のうちの何れか一つ以上を削除するとととともに、それを移動エージェント側に設けるようにしてもよい。

【００１２】

また、本発明によるプログラムを記録した記録媒体は、移動エージェントがプログラムコードの実行を行うエージェント実行処理（例えばステップＡ１，Ｃ１）と、乱数を出力する乱数生成処理（例えばステップＡ２，Ｃ２）と、乱数生成

処理で生成された乱数と移動エージェントの所有者の秘密鍵とを入力として、移動先のホストで移動エージェントが署名を計算するために必要な補助データを生成する部分署名補助データ生成処理（例えばステップＡ２，Ｃ３）と、計算されたデータの秘匿および署名の付与を行う公開鍵暗号計算処理（例えばステップＡ２，Ｃ４）とを実行するためのプログラムを記録したものである。

【００１３】

また、本発明による他のプログラムを記録した記録媒体は、移動エージェントがプログラムコードの実行を行うエージェント実行処理（例えばステップＡ１～Ａ６，Ａ１０～Ａ１３，Ｃ５～Ｃ８，Ｃ１９，Ｃ２３～Ｃ２５）と、署名対象データと移動エージェントが保有しているデータと移動先ホストの秘密鍵とを入力として移動エージェントが署名を計算するために必要なデータである部分署名を計算する部分署名計算処理（例えばステップＡ８，Ａ１４，Ｃ１１～Ｃ１７）と、移動先ホストによって計算された一つまたは複数の部分署名を入力として前記署名対象データに対する移動エージェントの所有者の秘密鍵を用いて計算を行ったディジタル署名を出力する部分署名署名化処理（例えばステップＡ１５，Ａ１６，Ｃ２６～Ｃ２８）と、計算されたデータの秘匿および移動先ホストの署名付与を行う公開鍵暗号計算処理（例えばステップＡ９，Ｃ１８～Ｃ２２）とを実行するためのプログラムを記録したものである。

【００１４】

また、本発明による他のプログラムを記録した記録媒体は、移動エージェントがプログラムコードの実行を行うエージェント実行処理（例えばステップＢ１～Ｂ７，Ｂ１２～Ｂ１４，Ｄ５～Ｄ８，Ｄ１９，Ｄ２３～Ｄ２５））と、乱数を出力する乱数生成処理（例えばステップＢ２，Ｄ２）と、乱数生成処理で生成された乱数を入力として、新規秘密鍵・公開鍵のペアと移動先のホストで移動エージェントが署名を計算するために必要な補助データを生成する部分署名補助データ生成処理（例えばステップＢ２，Ｄ３）と、計算されたデータの秘匿および署名の付与を行う公開鍵暗号計算処理（例えばステップＢ２，Ｄ４）とを実行するためのプログラムを記録したものである。

【００１５】

また、本発明による他の記録媒体は、移動エージェントがプログラムコードの実行を行うエージェント実行処理（例えばステップＢ１～Ｂ７，Ｂ１１～Ｂ１４，Ｄ５～Ｄ８，Ｄ１９，Ｄ２３～Ｄ２５）と、署名対象データと移動エージェントが保有しているデータと移動先ホストの秘密鍵とを入力として移動エージェントが署名を計算するために必要なデータである部分署名を計算する部分署名計算処理（例えばステップＢ９，Ｂ１５，Ｄ１１～Ｄ１７）と、移動先ホストによって計算された一つまたは複数の部分署名を入力として前記署名対象データに対するベースホストの部分署名補助データ生成処理で生成された前記新規秘密鍵を用いて計算を行ったディジタル署名を出力する部分署名署名化処理（例えばステップＢ１６，Ｂ１７，Ｄ２６～Ｄ２８）と、計算されたデータの秘匿および移動先ホストの署名付与を行う公開鍵暗号計算処理（例えばステップＢ１０，Ｄ１８～Ｄ２２）とを実行するためのプログラムを記録したものである。

【００１６】

前記ベースホストにおいては、公開鍵暗号計算手段により秘密鍵を用いて公開鍵暗号によるデータの暗号化、復号およびディジタル署名の計算を行うとともに、部分署名補助データ生成手段により乱数と秘密鍵を用いて移動先ホストｉが移動エージェントのディジタル署名を計算するために必要なデータを計算することによって移動エージェントが移動先のホストで必要となるデータの準備を行う。移動先ホストｉ（１≦ｉ≦ｋ）においては、部分署名計算手段が、移動してきた移動エージェントが移動中にディジタル署名を付与する事を決定したメッセージと前記部分署名補助データ生成手段の出力とを入力として、移動エージェントの所有者のディジタル署名を計算するために必要なデータである部分署名の計算を行うとともに、部分署名署名化手段が一つまたは複数の移動先ホストによって計算された部分署名を入力として、前記のメッセージに対する移動エージェント所有者のディジタル署名を出力する。また、過去に移動エージェントが移動してきた際に計算した部分署名の出力結果や、移動先ホストｉが移動エージェントから削除した部分署名補助データを格納するとともに、公開鍵暗号計算手段は、移動先ホストｉ（１≦ｉ≦ｋ）によって計算された部分署名や部分署名補助データ計算手段の秘匿および改竄防止のために暗号化およびディジタル署名の付与を行う

ことにより、エージェントの依頼に応じて必要なデータの計算を行う。

【００１７】

【発明の実施の形態】

以下、本発明の実施の形態を図面を参照して詳細に説明する。

図１は、本発明の第１の実施形態による移動エージェントによる署名計算システムの構成を示すブロック図である。

本署名計算システムは、ベースホスト１００と、移動先ホストｉ（１≦ｉ≦ｋ）と、移動エージェント１４０とを含んで構成される。図１では移動先ホストｉ（１≦ｉ≦ｋ）のうち、移動先ホスト１（１１０）と移動先ホスト２（１２０）と移動先ホストｋ（１３０）が図示されている。また図中の黒く塗りつぶされた矢印は移動エージェント１４０の移動を表しており、また矢印が破線になっている部分は、その破線部分で複数のホストを移動していることを表している。

【００１８】

次に、これらのホストと移動エージェントの概略的な構成及び動作について説明する。

ベースホスト１００は、乱数生成部１０１と、公開鍵暗号計算部１０２と、移動エージェントの所有者の秘密鍵である秘密鍵０（１０３）と、部分署名補助データ生成部１０４と、エージェント実行環境１０５とを含んで構成されている。

【００１９】

乱数生成部１０１は部分署名補助データ生成部１０４の要求を受け、乱数を出力する。公開鍵暗号計算部は１０２は、部分署名補助データ生成部１０４から受け渡されるデータを入力とし、この入力データの暗号化、復号、およびディジタル署名の計算を行う。ディジタル署名を計算する際には、公開鍵暗号計算部１０２には移動エージェント１４０の所有者の秘密鍵である秘密鍵０（１０３）も入力される。

【００２０】

部分署名補助データ生成部１０４は、前記乱数生成部１０１の出力と移動エージェント１４０の所有者の秘密鍵である秘密鍵０（１０３）とを入力とし、移動エージェント１４０が移動先ホストｉ（１≦ｉ≦ｋ）において、移動エージェン

ト１４０の所有者のディジタル署名を生成する際に必要なデータである部分署名を計算するための補助データを移動前の移動エージェント１４０内の中間データ格納部１４１に格納する。

エージェント実行環境１０５は、移動エージェント１４０がプログラム・コードの実行を行うためのＣＰＵ資源、メモリ等の計算環境を提供する。

【００２１】

移動先ホスト１（１１０）は、エージェント実行環境１１１と、部分署名計算部１１２と、部分署名署名化部１１３と、公開鍵暗号計算部１１４と、秘密鍵１（１１５）とデータ記憶部１１６とを含んで構成されている。

【００２２】

エージェント実行環境１１１は、前記エージェント実行環境１０５と同様に移動エージェント１４０がプログラム・コードの実行を行うためのＣＰＵ資源、メモリ等の計算環境を提供する。

【００２３】

部分署名計算部１１２は移動エージェント１４０が保持している部分署名補助データ生成部１０４の出力と移動エージェント１４０が複数の移動先ホストを移動している間に動的に決定された署名対象データと移動先ホスト１（１１０）の秘密鍵である秘密鍵１（１１５）とを入力として、移動エージェント１４０の所有者の秘密鍵である秘密鍵０（１０３）によるディジタル署名を計算するために必要なデータである部分署名を出力し、移動エージェント１４０内の中間データ格納部１４１に格納する。

【００２４】

部分署名署名化部１１３は、一つまたは複数の移動先ホストｉ（１≦ｉ≦ｋ）の部分署名計算部１１２、１２２、１３２によって出力され、移動エージェント１４０に格納された一つまたは複数の部分署名を入力として、移動エージェント１４０の所有者の秘密鍵である秘密鍵０（１０３）による前記署名対象データに対するディジタル署名を出力する。

【００２５】

公開鍵暗号計算部１１４は、前記部分署名計算部１１２の出力をディジタル署

名を渡すホスト以外に対して秘匿するために署名を渡すホストの公開鍵で該出力の暗号化を行う。また前記部分署名計算部１１２の出力を他の移動先ホストによって解析されたり改竄されることを防止するため、データを渡す相手の公開鍵による暗号化や移動ホスト１（１１０）の秘密鍵である秘密鍵１（１１５）を用いて前記部分署名計算部１１２の出力に対するディジタル署名の計算を行う。

【００２６】

データ記憶部１１６は、移動エージェント１４０が再び同一のホストに移動するまでの間一時的に後に必要となるデータの格納を行う。

移動先ホストｉ（２≦ｉ≦ｋ）の構成については、移動先ホスト１（１１０）の構成と同様であるため詳細な説明は省略する。

【００２７】

移動エージェント１４０は、中間データ格納部１４１を含んで構成されている。この中間データ格納部１４１は、ベースホスト１００の部分署名補助データ生成部１０４および移動先ホストｉ（１≦ｉ≦ｋ）の部分署名計算部によって出力されるディジタル署名の計算に必要となるデータの格納を行う。

【００２８】

本実施形態では、移動エージェント１４０が複数の移動先ホストを移動後に到達した移動先ホスト１（１１０）が提示したデータに対する移動エージェント１４０の所有者のディジタル署名を、移動先ホストｉ（１≦ｉ≦ｋ）が計算するデータから生成を行う。

【００２９】

次に図１および図２を参照して、本実施の形態による署名計算システムの全体の動作について詳細に説明する。

まず、署名を移動先のホストで計算する事を目的とした移動エージェント１４０がベースホスト１００内のエージェント実行環境１０５で起動される（図２のステップＡ１）。

【００３０】

次に、部分署名補助データ生成部１０４が移動エージェント１４０の所有者の秘密鍵である秘密鍵０（１０３）と、乱数生成部１０１から出力される一つまた

は複数の乱数とを入力として、秘密鍵０（１０３）と予め定められた関係を満足する部分署名補助データを生成して出力し、移動エージェント１４０内の中間データ格納部１４１に格納する。後に移動エージェント１４０が移動した先のホストで、部分署名補助データが改竄されないために、出力された部分署名補助データは秘密鍵０によってディジタル署名が施され、部分署名補助データとともに中間データ格納部１４１に格納される（ステップＡ２）。

【００３１】

移動エージェント１４０内の中間データ格納部１４１に部分署名補助データおよびディジタル署名が格納された後、移動エージェント１４０はネットワークを介して移動を開始する（ステップＡ３）。移動エージェント１４０は動的に０またはいくつかの移動先ホストを移動し、移動先のホストにデータを提示され、そのデータが署名を施す対象データであるかどうかの判断を行う（ステップＡ４）。

【００３２】

０またはいくつかの移動先ホストを動的に訪問後、移動エージェント１４０の移動中に動的に決定された移動先ホスト１（１１０）に移動し（ステップＡ５，Ａ６）、移動先ホスト１（１１０）からデータの提示を受ける。移動エージェント１４０は、移動先ホスト１（１１０）の提示したデータを署名対象データとして、移動エージェント１４０の所有者の秘密鍵である秘密鍵０（１０３）によるディジタル署名を計算する事を決定し、該署名対象データを移動エージェント１４０の中間データ格納部１４１に格納する（ステップＡ７）。

【００３３】

署名対象データ決定後、移動先ホスト１（１１０）は中間データ格納部１４１に格納されているデータの全部または一部と、移動先ホスト１（１１０）の秘密鍵である秘密鍵１（１１５）とを部分署名計算部１１２に入力する事によって、移動エージェント１４０の所有者の秘密鍵０による署名対象データに対する署名を計算する際に必要となる部分署名を得る（ステップＡ８）。

【００３４】

移動先ホスト１（１１０）は、部分署名計算部１１２に入力された中間データ

格納部１４１に格納されていたデータの中から以後に移動する移動先ホストｉ（２≦ｉ≦ｋ）で参照されないデータを中間データ格納部１４１から削除し、データ記憶部１１６に格納する。さらに部分署名計算部１１２の出力のうち以後に移動する移動先ホストｉ（１≦ｉ≦ｋ）で参照されないデータもデータ記憶部１１６に格納する。部分署名計算部１１２の出力のうち以後に移動する移動先ホストｉ（１≦ｉ≦ｋ）で参照されるデータは移動先ホスト１（１１０）の秘密鍵である秘密鍵１（１１５）によるディジタル署名を計算し、該署名とともに移動エージェント１４０内の中間データ格納部１４１に格納する（ステップＡ９）。

【００３５】

以上の処理が終了した後、移動エージェント１４０は次の移動先ホストである移動先ホスト２（１２０）に移動する（ステップＡ１０，Ａ１１，Ａ１２）。次に移動する移動先ホスト２（１２０）は、移動エージェント１４１が移動先ホスト１（１１０）に移動してきた時点で既に決定していたホストであっても、移動エージェント１４１が移動先ホスト１（１１０）に到着した後に移動先ホストによって動的に決定されたホストであっても良い。

【００３６】

以後に訪れる移動先ホストｉ（２≦ｉ≦ｋ）における処理の流れはｉの値に関わらず同様であるため、代表して移動先ホストｉ（１２０，１３０）における処理の流れに関して説明する。

移動先ホストｉ（１２０，１３０）は移動エージェント１４０の中間データ格納部１４１に格納されているデータの全部または一部と、移動先ホストｉ（１２０，１３０）の秘密鍵である秘密鍵ｉ（１２５，１３５）とを部分署名計算部１２２，１３２に入力する事によって移動エージェント１４０の所有者の秘密鍵０による署名対象データに対する署名を計算する際に必要となる部分署名を得る。このとき部分署名計算部１２２，１３２への入力となるデータに署名が付与されている場合には署名の検証を行う（ステップＡ８）。

【００３７】

移動先ホストｉ（１２０，１３０）は、部分署名計算部１２２，１３２に入力された移動エージェント１４０の中間データ格納部１４１に格納されていたデー

タのうち、以後に移動する移動先ホストｊ（ｊ＝１またはｉ＋１≦ｊ≦ｋ）で参照されないデータを公開鍵暗号計算部１２４，１３４に入力する事によって、移動エージェントの所有者の公開鍵で暗号化を行い、得られた暗号文を中間データ格納部１４１に格納する。

【００３８】

さらに部分署名計算部１２２，１３２の出力のうち移動先ホストｊ（ｉ＋１≦ｊ≦ｋ）で参照されないデータは公開鍵暗号計算部１２４，１３４を用いて移動先ホスト１（１１０）の公開鍵で暗号化を行い、得られた暗号文を中間データ格納部１４１に格納する。部分署名計算部１２２，１３２の出力のうち以後に移動する移動先ホストｊ（ｉ＋１≦ｊ≦ｋ）で参照されるデータは移動先ホストの秘密鍵である秘密鍵ｉ（１２５，１３５）によるディジタル署名を計算し、該署名とともに中間データ格納部１４１に格納する（ステップＡ９）。

【００３９】

以上の処理が終了した後、移動エージェント１４０は次の移動先ホストに移動する。次の移動先ホストはｉ＝ｋである場合には移動先ホスト１（１１０）となり、それ以外の場合には移動先ホストｉ＋１となる（ステップＡ１０，Ａ１１，Ａ１２，Ａ１３）。ｉ≠ｋの場合、次に移動する移動先ホストｉ＋１は、移動エージェント１４１が移動先ホストｉに移動してきた時点で既に決定していたホストであっても、移動エージェント１４１が移動先ホストｉに到着した後に移動先ホストによって動的に決定されたホストであっても良い。

【００４０】

移動エージェント１４０が再び移動先ホスト１（１１０）に移動した後、移動先ホスト１（１１０）は中間データ格納部１４１に格納されているデータの全部または一部と、移動先ホスト１（１１０）の秘密鍵である秘密鍵１（１１５）とを部分署名計算部１１２に入力する事によって、移動エージェント１４０の所有者の秘密鍵０による署名対象データに対するディジタル署名を計算する際に必要となる部分署名を得る（ステップＡ１４）。

【００４１】

部分署名計算後、移動先ホスト１（１１０）は中間データ格納部１４１に格納

されているデータに対して該データが暗号化されている場合は、該データと移動先ホスト１の秘密鍵である秘密鍵１（１１５）を公開鍵暗号計算部１１４に入力する事によって該データの復号を行った後、復号したデータとディジタル署名を生成したホストの公開鍵を公開鍵暗号計算部１１４に入力する事によって該復号データに対する署名の検証を行い、該データが暗号化されていない場合は、該データとディジタル署名を生成したホストの公開鍵を公開鍵暗号計算部１１４に入力し、該データに対する署名の検証を行う事によってデータの改竄が行われていない事を確認する（ステップＡ１５）。

【００４２】

全てのディジタル署名の検証が終了した時点において、移動先ホスト１（１１０）は移動先ホストｉ（１≦ｉ≦ｋ）によって計算された部分署名が得られる。移動先ホスト１（１１０）は得られた全てまたは一部の部分署名を部分署名署名化部１１３に入力する事によって、前記署名対象データに対して移動エージェントの所有者の秘密鍵である秘密鍵０によるディジタル署名が出力として得られる（ステップＡ１６）。移動先ホスト１（１１０）は得られたディジタル署名をデータ記憶部１１６に格納し、移動エージェント１４０はベースホスト１００に戻る（ステップＡ１７）。

【００４３】

次に、本実施の形態による効果について説明する。

以上の処理によって得られたディジタル署名は、移動エージェント１４０が移動したホストや移動した順序によらず、常に移動エージェントの所有者の公開鍵によって正当性が検証できるディジタル署名になっている。署名の偽造の可能性に関しては、移動エージェントの所有者の署名を生成するために、ｋ個の移動先ホストの秘密鍵による演算が必要になるため、ｋ個の移動先ホストが結託しない限りは署名の偽造を行う事を困難にすることができる。

【００４４】

次に本発明の第２の実施の形態について説明する。

前述した第１の実施の形態では、移動エージェントが計算する署名が、移動先ホストが提示した署名対象データに対して移動エージェントの所有者の秘密鍵を

用いて計算した署名であったのに対し、本発明の第２の実施の形態では、移動エージェントが計算する署名が、移動エージェントのベースホストによって移動エージェントが移動を始める前に新規に生成された秘密鍵を用いて署名対象データに対して計算されたディジタル署名と、該ベースホストが新規に作成した秘密鍵に対応する公開鍵と、該公開鍵に対する移動エージェントの所有が予め所有している秘密鍵を用いて計算したディジタル署名のデータの三つ組みとなる点において異なっている。

【００４５】

図３は、本発明の第２の実施形態による署名計算システムの構成を示すブロック図である。

本署名計算システムは、ベースホスト３００と、移動先ホストｉ（１≦ｉ≦ｋ）と、移動エージェント３４０とを含んで構成される。図３では移動先ホストｉ（１≦ｉ≦ｋ）のうち、移動先ホスト１（３１０）と、移動先ホスト２（３２０）と、移動先ホストｋ（３３０）が図示されている。また図中の黒く塗りつぶされた矢印は移動エージェント３４０の移動を表しており、また矢印が破線になっている部分は、その破線部分で複数のホストを移動していることを表している。

【００４６】

次にこれらのホストと移動エージェントの構成および動作について概略的に説明する。

ベースホスト３００は、乱数生成部３０１と、公開鍵暗号計算部３０２と、移動エージェント３４０の所有者の秘密鍵である秘密鍵０（３０３）と、部分署名補助データ生成部３０４と、エージェント実行環境３０５とを含んで構成されている。

上記構成要素のうち、乱数生成部３０１、公開鍵暗号計算部３０２、秘密鍵０（３０３）、エージェント実行環境３０５については、第１の実施形態における乱数生成部１０１、公開鍵暗号計算部１０２、秘密鍵０（１０３）、エージント実行環境１０５とそれぞれ同一の動作であるため詳細な説明は省略する。

【００４７】

部分署名補助データ生成部３０４は、前記乱数生成部３０１の出力を入力とし

、新規の秘密鍵と公開鍵の組の生成、移動エージェント３４０が移動先ホストｉ（１≦ｉ≦ｋ）において、前記の新規秘密鍵によるディジタル署名を生成するために必要となる部分署名を計算するための補助データを該データに対する移動エージェント３４０所有者の秘密鍵である秘密鍵０（３０３）によるディジタル署名とともに移動前の移動エージェント３４０内の中間データ格納部３４１へ格納する事、および前記の新規公開鍵を移動エージェント３４０所有者の秘密鍵である秘密鍵０（３０３）によるディジタル署名とともに移動前の移動エージェント３４０内の中間データ格納部３４１へ格納する事を行う。

【００４８】

移動先ホスト１（３１０）は、エージェント実行環境３１１と、部分署名計算部３１２と部分署名署名化部３１３と公開鍵暗号計算部３１４とデータ記憶部３１６とを含んで構成されている。

上記構成要素のうち、エージェント実行環境３１１、部分署名計算部３１２、公開鍵暗号計算部３１４、データ記憶部３１６については、第１の実施形態におけるエージェント実行環境１１１、部分署名計算部１１２、公開鍵暗号計算部１１４、データ記憶部１１６とそれぞれ同一な動作であるため詳細な説明は省略する。

【００４９】

部分署名署名化部３１３は一つまたは複数の移動先ホストｉ（１≦ｉ≦ｋ）の部分署名計算部３１２、３２２、３３２によって出力され、移動エージェント３４０に格納された一つまたは複数のデータを入力として、ベースホスト３００の部分署名補助データ生成部３０４によって生成された新規秘密鍵によるディジタル署名と、中間データ格納部３４１に格納されている新規公開鍵と、該新規公開鍵に対する移動エージェント３４０所有者の秘密鍵である秘密鍵０（３０３）によるディジタル署名とを組にして移動エージェント３４０の所有者のディジタル署名として出力する。

移動先ホストｉ（２≦ｉ≦ｋ）および移動エージェント３４０の構成については、移動先ホスト１の構成と同じであるため詳細な説明は省略する。

【００５０】

本実施形態では、移動エージェント３４０が複数の移動先ホストを移動後に到達した移動先ホスト１（３１０）が提示したデータに対する移動エージェント３４０の所有者のディジタル署名を、移動先ホストｉ（１≦ｉ≦ｋ）が計算するデータから生成する。

【００５１】

次に図３および図４を参照して本実施の形態による署名計算システムの全体の動作について詳細に説明する。

まず、署名を移動先のホストで計算する事を目的とした移動エージェント３４０がベースホスト３００内のエージェント実行環境３０５で起動される（図４のステップＢ１）。

【００５２】

次に、部分署名補助データ生成部３０４は乱数出力部３０１から出力される一つまたは複数の乱数を入力として新規に公開鍵と秘密鍵のペアを計算する。該公開鍵に対しては移動エージェント３４０の秘密鍵である秘密鍵０によるディジタル署名を計算し、署名とともに移動エージェント３４０内の中間データ格納部３４１に格納する（ステップＢ２）。

【００５３】

次に部分署名補助データ生成部３０４は、乱数生成部３０１から出力される一つまたは複数の乱数とを入力として、ステップＢ２で生成した新規秘密鍵と予め定められた関係を満足する部分署名補助データを出力し、中間データ格納部３４１に格納する。後に移動エージェント３４０が移動した先のホストで部分署名補助データが改竄されないために、出力された部分署名補助データは秘密鍵０によるディジタル署名が施され、部分署名補助データとともに中間データ格納部３４１に格納される（ステップＢ３）。

【００５４】

中間データ格納部３４１に部分署名補助データおよびディジタル署名が格納された後、移動エージェント３４０はネットワークを介して移動を開始する（図４のステップＢ４）。移動エージェント３４０は動的に０またはくつかの移動先ホストを移動し、移動先のホストにデータを提示され、そのデータが署名を施す対

象データであるかどうかの判断を行う（ステップＢ５）。

【００５５】

０またはいくつかの移動先ホストを動的に訪問後、移動エージェント３４０の移動中に動的に決定された移動先ホスト１（３１０）に移動し（ステップＢ６，Ｂ７）、移動先ホスト１（３１０）からデータの提示を受ける。移動エージェント３４０は、移動先ホスト１（３１０）の提示したデータを署名対象データとして、前記ベースホスト３００の部分署名補助データ生成部３０４によって生成された新規秘密鍵によるディジタル署名を計算する事を決定し、該署名対象データを中間データ格納部３４１に格納する（ステップＢ８）。

【００５６】

署名対象データ決定後、移動先ホスト１（３１０）は中間データ格納部３４１に格納されているデータの全部または一部と、移動先ホスト１（３１０）の秘密鍵である秘密鍵１（３１５）とを部分署名計算部３１２に入力する事によって前記ベースホスト３００の部分署名補助データ生成部３０４によって生成された新規秘密鍵による署名対象データに対する署名を計算する際に必要となる部分署名を得る。このとき部分署名入力部３２２，３３２への入力となるデータに署名が付与されている場合には署名の検証を行う（ステップＢ９）。

【００５７】

移動先ホスト１（３１０）は、部分署名計算部３１２に入力された中間データ格納部３４１に格納されていたデータの中から以後に移動する移動先ホストｉ（２≦ｉ≦ｋ）で参照されないデータを該中間データ格納部３４１から削除し、データ記憶部３１６に格納する。さらに部分署名計算部３１２の出力のうち以後に移動する移動先ホストｉ（１≦ｉ≦ｋ）で参照されないデータもデータ記憶部３１６に格納する。部分署名計算部３１２の出力のうち以後に移動する移動先ホストｉ（１≦ｉ≦ｋ）で参照されるデータは移動先ホスト１（３１０）の秘密鍵である秘密鍵１（３１５）によるディジタル署名を計算し該署名とともに中間データ格納部３４１に格納する（ステップＢ１０）。

【００５８】

以上の処理が終了した後、移動エージェント３４０は次の移動先ホストである

移動先ホスト２（３２０）に移動する（ステップＢ１１，Ｂ１２，Ｂ１３）。次に移動する移動先ホスト２（３２０）は、移動エージェント３４１が移動先ホスト１（３１０）に移動してきた時点で既に決定していたホストであっても、移動エージェント３４１が移動先ホスト１（３１０）に到着した後に移動先ホストによって動的に決定されたホストであっても良い。

【００５９】

以後に訪れる、移動先ホストｉ（２≦ｉ≦ｋ）における処理の流れはｉの値に関わらず同様であるため、代表して移動先ホストｉ（３２０，３３０）における処理の流れに関して説明する。

移動先ホストｉ（３２０，３３０）は移動エージェント３４０の中間データ格納部３４１に格納されているデータの全部または一部と、移動先ホストｉ（３２０，３３０）の秘密鍵である秘密鍵ｉ　３２５，３３５とを部分署名計算部３２２，３３２に入力する事によって前記ベースホスト３００の部分署名補助データ生成部３０４によって生成された新規秘密鍵による署名対象データに対するディジタル署名を計算する際に必要となる部分署名を得る（ステップＢ９）。

【００６０】

移動先ホストｉ（３２０，３３０）は、部分署名計算部３２２，３３２に入力された中間データ格納部３４１に格納されていたデータのち、以後に移動する移動先ホストｊ（ｊ＝１またはｉ＋１≦ｊ≦ｋ）で参照されないデータを公開鍵暗号計算部３２４，３３４に入力する事によって、移動エージェント３４０の所有者の公開鍵で暗号化を行い、得られた暗号文を中間データ格納部３４１に格納する。さらに部分署名計算部３２２，３３２の出力のうち以後に移動する移動先ホストｊ（ｉ＋１≦ｊ≦ｋ）で参照されないデータも公開鍵暗号計算部３２４，３３４を用いて移動先ホスト１（３１０）の公開鍵で暗号化を行い、暗号文を中間データ格納部３４１に格納する。

【００６１】

部分署名計算部３２２，３３２の出力のうち以後に移動する移動先ホストｊ（ｉ＋１≦ｊ≦ｋ）で参照されるデータは移動先ホストの秘密鍵である秘密鍵ｉ３２５，３３５によってディジタル署名を計算し該署名とともに中間データ格納部

３４１に格納する（ステップＢ１０）。

【００６２】

以上の処理が終了した後、移動エージェント３４０は次の移動先ホストに移動する。次の移動先ホストはｉ＝ｋである場合には移動先ホスト１（３１０）となり、それ以外の場合には移動先ホストｉ＋１となる（ステップＢ１１，Ｂ１２，Ａ１３，Ｂ１４）。ｉ≠ｋの場合、次に移動する移動先ホストｉ＋１は、移動エージェント３４０が移動先ホストｉに移動してきた時点で既に決定していたホストであっても、移動エージェント３４０が移動先ホストｉに到着した後に移動先ホストによって動的に決定されたホストであっても良い。

【００６３】

移動エージェント３４０が再び移動先ホスト１　３１０に移動した後、移動先ホスト１（３１０）は中間データ格納部３４１に格納されているデータの全部または一部と、移動先ホスト１（３１０）の秘密鍵である秘密鍵１（３１５）とを部分署名計算部３１２に入力する事によって前記ベースホスト３００の部分署名補助データ生成部３０４によって生成された新規秘密鍵による署名対象データに対するディジタル署名を計算する際に必要となる部分署名を得る（ステップＢ１５）。

【００６４】

部分署名計算後、移動先ホスト１（３１０）は中間データ格納部３４１に格納されているデータに対して該データが暗号化されている場合は該データと移動先ホスト１（３１０）の秘密鍵である秘密鍵１（３１５）を公開鍵暗号計算部３１４に入力する事によって該データの復号を行った後、復号したデータとディジタル署名を生成したホストの公開鍵を公開鍵暗号計算部３１４に入力する事によって該復号データに対する署名の検証を行い、該データが暗号化されていない場合は該データと署名を生成したホストの公開鍵を公開鍵暗号計算部３１４に入力するし、該データに対する署名の検証を行う事によってデータの改竄が行われていない事を確認する（ステップＢ１６）。

【００６５】

全ての署名の検証が終了した時点において、移動先ホスト１（３１０）は移動

先ホストｉ（１≦ｉ≦ｋ）によって計算された部分署名が得られる。移動先ホスト１は得られた部分署名の全てまたは一部を部分署名署名化部３１３に入力する事によって、前記署名対象データに対して前記ベースホスト３００の部分署名補助データ生成部３０４によって生成された新規秘密鍵によるディジタル署名が出力として得られる（ステップＢ１７）。

【００６６】

移動先ホスト１（３１０）は得られたディジタル署名と、前記ベースホスト３００の部分署名補助データ生成部３０４によって移動エージェント３４０内の中間データ格納部３４１に格納された新規公開鍵と該新規公開鍵に対する移動エージェント３４０の所有者の秘密鍵である秘密鍵０を用いて計算したディジタル署名をデータ記憶部３１６に格納し、移動エージェント３４０はベースホスト３００に戻る（ステップＢ１８）。

【００６７】

次に、本実施の形態による効果について説明する。

以上の処理によって得られたディジタル署名は、移動エージェントが移動したホストや移動した順序によらず、常に移動エージェントの所有者の公開鍵によって正当性が検証できる署名になっている。署名の偽造可能性に関しては、移動エージェントの所有者の署名を生成するために、ｋ個の移動先ホストの秘密鍵による演算が必要になるため、ｋ個の移動先ホストが結託しない限りは署名の偽造を行う事を困難にすることができる。更にｋ個のホストが結託した場合でも、明らかになる情報はベースホストが新規に生成する秘密鍵だけであるので、ベースホストの所有者の秘密鍵は結託した悪意のある移動ホストに知られる事はない。

【００６８】

次に本発明の第３の実施の形態について説明する。

第３の実施の形態は、前述した第１の実施の形態において、移動先ホストｉ（１≦ｉ≦ｋ）に存在していた部分署名計算部１１２，１２２，１３２が移動エージェント１４０のプログラム・コードによって実現されている点において異なる。

【００６９】

第３の実施の形態においては、移動エージェント１４０のプログラム・コードの入力として移動先ホストｉ（１≦ｉ≦ｋ）の秘密鍵が与えられるため、該秘密鍵を移動エージェント１４０の所有者および別の移動先ホストに知られないようにするために、移動エージェント１４０のプログラム・コードおよび中間データ格納手段に格納されている該秘密鍵の情報を移動エージェント１４０が次のホストに移動する前に消去する必要がある。

【００７０】

次に本発明の第４の実施の形態について説明する。

第４の実施の形態は、第１の実施の形態において、移動先ホストに存在していた部分署名署名化部１１３，１２３，１３３が移動エージェント１４０のプログラム・コードによって実現されている点において異なる。

【００７１】

次に本発明の第５の実施の形態について説明する。

第５の実施の形態は、第１の実施の形態において、移動先ホストｉ（１≦ｉ≦ｋ）に存在していた公開鍵暗号計算部１１４，１２４，１３４が移動エージェント１４０のプログラム・コードによって実現されている点において異なる。

【００７２】

次に本発明の第６の実施の形態について説明する。

第６の実施の形態は、第１の実施の形態において、移動先ホストｉ（１≦ｉ≦ｋ）に存在していた部分署名計算部１１２，１２２，１３２および部分署名署名化部１１３，１２３，１３３が移動エージェント１４０のプログラム・コードによって実現されている点において異なる。

【００７３】

次に本発明の第７の実施の形態について説明する。

第７の実施の形態は、第１の実施の形態において、移動先ホストｉ（１≦ｉ≦ｋ）に存在していた部分署名署名化部１１３，１２３，１３３および公開鍵暗号計算部１１４，１２４，１３４が移動エージェント１４０のプログラム・コードによって実現されている点において異なる。

【００７４】

次に本発明の第８の実施の形態について説明する。

第８の実施の形態は、第１の実施の形態において、移動先ホストｉ（１≦ｉ≦ｋ）に存在していた部分署名計算部１１２，１２２，１３２および公開鍵暗号計算部１１４，１２４，１３４が移動エージェント１４０のプログラム・コードによって実現されている点において異なる。

【００７５】

次に本発明の第９の実施の形態について説明する。

第９の実施の形態は、第１の実施の形態において、移動先ホストｉ（１≦ｉ≦ｋ）に存在していた部分署名計算部１１２，１２２，１３２および部分署名署名化部１１３，１２３，１３３および公開鍵暗号計算部１１４，１２４，１３４が移動エージェント１４０のプログラム・コードによって実現されている点において異なる。

【００７６】

次に本発明の第１０の実施の形態について説明する。

第１０の実施の形態は、前述した第２の実施の形態において、移動先ホストｉ（１≦ｉ≦ｋ）に存在していた部分署名計算部１１２，１２２，１３２が移動エージェント１４０のプログラム・コードによって実現されている点において異なる。

【００７７】

上述した第５～第１０の実施の形態においては、移動エージェント１４０のプログラム・コードの入力として移動先ホストｉ（１≦ｉ≦ｋ）の秘密鍵が与えられるため、該秘密鍵を移動エージェント１４０の所有者および別の移動先ホストに知られないようにするために、移動エージェント１４０のプログラム・コードおよび中間データ格納手段に格納されている該秘密鍵の情報を移動エージェント１４０が次のホストに移動する前に消去する必要がある。

【００７８】

次に本発明の第１１の実施の形態について説明する。

第１１の実施の形態は、第２の実施の形態において、移動先ホストｉ（１≦ｉ≦ｋ）に存在していた部分署名署名化部１１３，１２３，１３３が移動エージェ

ント１４０のプログラム・コードによって実現されている点において異なる。

【００７９】

次に本発明の第１２の実施の形態について説明する。

第１２の実施の形態は、第２の実施の形態において、移動先ホストｉ（１≦ｉ≦ｋ）に存在していた公開鍵暗号計算部１１４，１２４，１３４が移動エージェント１４０のプログラム・コードによって実現されている点において異なる。

【００８０】

次に本発明の第１３の実施の形態について説明する。

第１３の実施の形態は、第２の実施の形態において、移動先ホストｉ（１≦ｉ≦ｋ）に存在していた部分署名計算部段１１２，１２２，１３２および部分署名署名化部１１３，１２３，１３３が移動エージェント１４０のプログラム・コードによって実現されている点において異なる。

【００８１】

次に本発明の第１４の実施の形態について説明する。

第１４の実施の形態は、第２の実施の形態において、移動先ホストｉ（１≦ｉ≦ｋ）に存在していた部分署名署名化部１１３，１２３，１３３および公開鍵暗号計算部１１４，１２４，１３４が移動エージェント１４０のプログラム・コードによって実現されている点において異なる。

【００８２】

次に本発明の第１５の実施の形態について説明する。

第１５の実施の形態は、第２の実施の形態において、移動先ホストｉ（１≦ｉ≦ｋ）に存在していた部分署名計算部１１２，１２２，１３２および公開鍵暗号計算部１１４，１２４，１３４が移動エージェント１４０のプログラム・コードによって実現されている点において異なる。

【００８３】

次に本発明の第１６の実施の形態について説明する。

第１６の実施の形態は、第２の実施の形態において、移動先ホストｉ（１≦ｉ≦ｋ）に存在していた部分署名計算部１１２，１２２，１３２および部分署名署名化部１１３，１２３，１３３および公開鍵暗号計算部１１４，１２４，１３４

が移動エージェント１４０のプログラム・コードによって実現されている点において異なる。

【００８４】

本発明の第１２～１６の実施の形態においては、移動エージェント１４０のプログラム・コードの入力として移動先ホストｉ（１≦ｉ≦ｋ）の秘密鍵が与えられるため、該秘密鍵を移動エージェント１４０の所有者および別の移動先ホストに知られないようにするために、移動エージェント１４０のプログラム・コードおよび中間データ格納手段に格納されている該秘密鍵の情報を移動エージェント１４０が次のホストに移動する前に消去する必要がある。

【００８５】

第３～１６の実施の形態は、要するに第１、第２の実施の形態において、移動先ホストにおける部分署名部、部分署名署名化部、公開鍵暗号計算部のうちの何れか一つ以上を除くとともに、その除いたものを移動エージェント側に設けたものである。

【００８６】

【実施例】

次に、本発明の具体的な実施例を図面を参照して説明する。

図５および図６は第１の実施例を示すブロック図である。

本実施例は、前述の第１の実施の形態による署名計算方式をＲＳＡ署名方式対応とするものである。

ＲＳＡ署名方式は『「Ｈａｎｄｂｏｏｋ ｏｆ Ａｐｐｌｉｅｄ Ｃｒｙｐｔｏｇｒａｐｈｙ」（Ａ．Ｍｅｎｅｚｅｓ，Ｐ．Ｏｏｒｓｃｈｏｔ，Ｓ．Ｖａｎｓｔｏｎｅ著，ＣＲＣ Ｐｒｅｓｓ，１９９７，ＩＳＢＮ ０－８４９３－８５２３－７）ｐｐ．４３３－４３８』に詳しく述べられている。

【００８７】

ここでは本実施例で用いる情報セキュリティの実現方式であるＲＳＡ署名方式，（ｋ，ｎ）閾値秘密分散共有法，ＥｌＧａｍａｌ暗号方式について簡単に説明する。

まずＲＳＡ署名方式について簡単に説明する。

ＲＳＡ署名方式は５１２ビット程度の二つの素数ｐ，ｑの積ｎと、ｌｃｍ（ｐ－１，ｑ－１）（ここでｌｃｍ（ａ，ｂ）はａとｂの最小公倍数を表すものとする）と互いに素である数ｅとの組（ｎ，ｅ）を公開鍵として持ち、ｅｄ＝１　（ｍｏｄ　ｌｃｍ（ｐ－１，ｑ－１））を満足するｄを秘密鍵として持つ。

【００８８】

Ｍを署名を計算したいメッセージとすると、Ｍに対する署名Ｓは

$S=M^{d}$　（ｍｏｄ　ｎ）

で表される。また、メッセージと署名のペア（Ｍ，Ｓ）を受信した受信者は、（Ｍ，Ｓ）が式

$M=S^{e}$　（ｍｏｄ　ｎ）

を満足する事を確かめる事により、メッセージの正当性を検証する。

【００８９】

次に（ｋ，ｎ）閾値秘密分散共有法について簡単に説明する。

（ｋ，ｎ）閾値秘密分散法は秘密Ｓを次の（１），（２）の条件を満足するようにｎ人の参加者に秘密に関する分散情報を配布する方式である。

（１）ｋ人未満の参加者が集まって自分の保有する分散情報を公開しても秘密Ｓに関する情報は全く得られない。

（２）ｋ人以上の参加者が集まって自分の保有する分散情報を公開すると秘密Ｓは一意に復元される。

【００９０】

（ｋ，ｎ）閾値秘密分散共有法の実現方式に関しては『「Ｈａｎｄｂｏｏｋ　ｏｆ　Ａｐｐｌｉｅｄ　Ｃｒｙｐｔｏｇｒａｐｈｙ」（Ａ．Ｍｅｎｅｚｅｓ，Ｐ．Ｏｏｒｓｃｈｏｔ，Ｓ．Ｖａｎｓｔｏｎｅ著，ＣＲＣ　Ｐｒｅｓｓ，１９９７，ＩＳＢＮ　０－８４９３－８５２３－７）ｐｐ．５２５－５２６』に詳しく述べられている。

【００９１】

ここでは多項式を用いた実現方式について簡単に説明する。

分散共有したい秘密Ｓ（$1 \leqq S < q$，ｑ：素数）に対して、信頼できる第三者は以下のような多項式ｆ（ｘ）をランダムに選ぶ。

$f(x) = S + a_1 x + a_2 x^2 + \cdots\cdots + a_{k-1} x^{k-1} \pmod{q}$

次に各参加者ｉ（１≦ｉ＜ｎ）に分散情報としてｖｉ＝ｆ（ｉ）を渡す。

【００９２】

上述のように分散情報を定めると、上記（１），（２）の性質がともに満たされる。ｋ人の参加者ｉ１，ｉ２，…，ｉｋが集まって自分の分散情報ｖｉ１，ｖｉ２，…，ｖｉｋを公開した場合、秘密Ｓは次式に従って復元される。

【００９３】

【数１】

$$S = \sum_{j=1}^{k} L_{ij} v_{ij} \pmod{q}$$

【００９４】

但しL_{ij}は次式で表される。

【００９５】

【数２】

$$L_{ij} = \prod_{1 \leqq j \leqq k,\ i \neq j} \frac{i_i}{i_i - i_j} \pmod{q}$$

【００９６】

次にＥｌＧａｍａｌ暗号方式について説明する。

ＥｌＧａｍａｌ暗号方式は『「Ｈａｎｄｂｏｏｋ　ｏｆ　Ａｐｐｌｉｅｄ　Ｃｒｙｐｔｏｇｒａｐｈｙ」（Ａ．Ｍｅｎｅｚｅｓ，Ｐ．Ｏｏｒｓｃｈｏｔ，Ｓ．Ｖａｎｓｔｏｎｅ著，ＣＲＣ　Ｐｒｅｓｓ，１９９７，ＩＳＢＮ　０－８４９３－８５２３－７）ｐｐ．２９４－２９８』に詳しく述べられている。

【００９７】

ここではＥｌＧａｍａｌ暗号方式の公開鍵、秘密鍵、暗号化法、復号法について簡単に説明する。

ＥｌＧａｍａｌ暗号方式は、５１２ビット程度の素数ｐと、法ｐの巡回群の生成元ｇを共通パラメータとして持ち、秘密鍵ｘ（０≦ｘ＜ｐ）を秘密鍵として持

ち、

$y = g^x \pmod p$

を公開鍵として持つ。

【００９８】

ｍを暗号化したいメッセージとすると、送信者は乱数ｒを選び、受信者の公開鍵ｙを用いて$G = g^r$，$M = m y^r$を計算し、（Ｇ，Ｍ）を暗号文として受信者に送る。暗号文（Ｇ，Ｍ）を受信した受信者は、自分の秘密鍵ｘを用いて$m = M / G^x$を計算する事によりメッセージを復号する。

【００９９】

本実施例では、移動エージェントの所有者はＲＳＡ秘密鍵d_Aおよび対応する公開鍵ｅＡ を所有している。また移動先ホストｉ（１≦ｉ≦ｎ）もＲＳＡ秘密鍵ｄｉ および対応する公開鍵ｅｉ を所有している。

【０１００】

さらに本方式全体にはｋ個のＥｌＧａｍａｌ暗号公開鍵y_i（$1 \leqq i < k$）が存在し、対応する秘密鍵x_i（$1 \leqq i < k$）は（ｉ＋１，ｎ）閾値秘密分散共有法を用いて各移動先ホストｊ（１≦ｊ≦ｎ）に秘密鍵として分散共有されている。以後、移動先ホストｊ（１≦ｊ≦ｎ）が保有する秘密鍵ｘｉ に対する分散情報をｖｉｊと表記する。このときｘｉ を分散するのに用いた多項式ｆｉ （ｘ）に対して、

$v_{ij} = f_i(j)$

が成立している。

【０１０１】

以上の準備の下、図５および図６を参照して本実施例の処理の流れについて説明する。

まずベースホスト５００において移動エージェント５４０が起動される（図６のステップＣ１）。

【０１０２】

部分署名補助データ生成部５０４は秘密鍵d_Aと乱数生成手段５０１から出力される乱数を入力として

【０１０３】

【数３】

$$d_A = \sum_{i=1}^{k-1} r_i \pmod{lcm(p-1, q-1)}$$

【０１０４】

を満足する乱数ｒｉ　（１≦ｉ＜ｋ）を生成する（ステップＣ２）。得られたｒｉ

に対してはｄＡ による署名が計算され（ステップＣ３）、さらにＥｌＧａｍａｌ暗号公開鍵ｙｉ を用いて暗号文（Ｇｉ，Ｍｉ）が計算された後（ステップＣ４）、暗号文（Ｇｉ，Ｍｉ）およびｒｉ に対する署名は移動エージェント５４０の中間データ格納部５４１に格納される。

【０１０５】

部分署名の計算に必要な補助データを中間データ格納部５４１に格納した後、移動エージェント５４０は移動を開始し（ステップＣ５）、いくつかの移動先ホストを動的に巡回した後（ステップＣ６）、ホスト移動中に動的に決定された移動先ホスト１（５１０）に移動し（ステップＣ７，Ｃ８）、移動先ホスト１（５１０）が提示したデータｍに対して署名を計算する事を決定する（ステップＣ９）。

【０１０６】

提示したデータｍに移動エージェント５４０が署名を計算する事を決定した後、移動先ホスト１（５１０）はステップＣ４でベースホスト５００によって計算され中間データ格納部５４１に格納されている暗号文（Ｇｉ，Ｍｉ）（１≦ｉ＜ｋ）を部分署名計算部５１３に入力する事によってＧｉ１を次式に従って計算する（ステップＣ１０）。

【０１０７】

【数４】

$$G_{i1} = G_i^{V_{i1}} \pmod{p}$$

【０１０８】

Ｇｉ１（１≦ｉ＜ｋ）を計算した後、更に移動先ホスト１（５１０）は公開鍵暗号計算部５１４に、Ｇｉ１と移動先ホスト１（５１０）の秘密鍵ｄ１（５１５）を入力する事により、ステップＣ１０で計算したＧｉ１に対する移動先ホスト１（５１０）のＲＳＡディジタル署名を計算する（ステップＣ１１）。署名計算後、移動先ホスト１（５１０）はＧｋ－１１を移動先ホスト１（５１０）のデータ記憶部５１６に格納し（ステップＣ１２）、残りの計算結果Ｇｉ１（１≦ｉ＜ｋ－１）を移動エージェント５４０の中間データ格納部５４１に格納する（ステップＣ１３）。中間データ格納部５４１にデータ格納をした後、移動エージェント５４０は次の移動先ホストである移動先ホスト２（５２０）に移動する（ステップＣ１４，Ｃ１５）。

【０１０９】

移動エージェント５４０が移動先ホストｉ（２≦ｉ≦ｋ）に移動すると、移動先ホストｉはステップＣ４でベースホスト５００によって計算され中間データ格納部５４１に格納されている暗号文（Ｇｊ，Ｍｊ）（ｉ－１≦ｊ＜ｋ）を部分署名計算部に入力する事によってＧｊｉを次式に従って計算する（ステップＣ１６）。

【０１１０】

【数５】

$$G_{ji} = G_j^{V_{ji}} \pmod{p}$$

【０１１１】

Ｇｊｉ（ｉ－１≦ｊ＜ｋ）を計算した後、移動先ホストｉは、計算したＧｊｉと移動先ホストｉの秘密鍵ｄｉを公開鍵暗号計算部に入力する事によってＧｊ

ｉに対する移動先ホストｉのＲＳＡ署名を計算し（ステップＣ１７）、さらにG_{k-1i}を署名対象データの提示を行った移動先ホスト１（５１０）の公開鍵ｅ１で暗号化する（ステップＣ１８）。ここで現在移動エージェント５４０が訪問している移動先ホストが移動先ホストｋ（移動先ホスト１を訪問後ｋ番目に訪問したホスト）であった場合には、移動エージェント５４０は移動先ホスト１に戻る（ステップＣ１９，２５）。

【０１１２】

現在の移動先ホストが移動先ホストｋでない場合、この時点において、移動先ホストｉはG_{i-11}，G_{i-12}，G_{i-13}，…，G_{i-1i}というｉ個のG_{i-1j}（１≦ｊ≦ｉ）なるデータを保有している。

【０１１３】

【数６】

$$G_{i-1j} = G_{j-1}^{V_{i-1j}} \pmod{p}$$

【０１１４】

という関係とv_{i-1j}が（ｉ，ｎ）閾値秘密分散共有法の部分情報である事に注意すると、

【０１１５】

【数７】

$$\prod_{j=1}^{i} G_{i-1j}^{L_j} = G_{i-1}^{\sum_{j=1}^{i} L_j v_{i-1j}} = G_{i-1}^{x_{i-1}} \pmod{p}$$

【０１１６】

が成立する。ＥｌＧａｍａｌ暗号の復号法と比較すると、

【０１１７】

【数８】

$$r_{i-1} = \frac{M_{i-1}}{\prod_{j=1}^{i} G_{i-1j}^{L_j}} = \frac{M_{i-1}}{G_{i-1}^{x_{i-1}}} \pmod{p}$$

【０１１８】

が成立するので、部分署名計算部にG_{i-11}，G_{i-12}，G_{i-13}，…，Ｇｉ－１ｉを入力して上記計算を行う事によって、r_{i-1}が得られる。さらに部分署名部はｍを入力として得る事により部分署名

【０１１９】

【数９】

$$S_{i-1} = m^{r_{i-1}} \pmod{n}$$

【０１２０】

を出力する（ステップＣ２０）。

S_{i-1}が出力された後、移動先ホストｉはS_{i-1}と移動先ホスト１の公開鍵ｅ１とを公開鍵暗号計算部に入力してS_{i-1}を暗号化し、さらにS_{i-1}と移動エージェント５４０の所有者の公開鍵ｄｉを公開鍵暗号計算部に入力して、S_{i-1}に対する移動先ホストｉのＲＳＡ署名を計算し、得られた暗号文および署名を移動エージェント５４０の中間データ格納部５４１に格納する（ステップＣ２１）。

【０１２１】

さらに以後の訪問先ホストで参照される事のないデータであるG_{i-1j}（１≦ｊ≦ｉ）と移動エージェント５４０の所有者の公開鍵ｅＡを公開鍵暗号計算部に入力する事によって得られるG_{i-1j}に対するＲＳＡ暗号文を中間データ格納部５４１に格納する（ステップＣ２２）。この暗号文データは、後にベースホスト５００に戻った移動エージェント５４０が行ってきた計算を移動エージェント５４０の所有者が検証するために用いられる。

【０１２２】

移動先ホストｉによって計算されたデータが中間データ格納部５４１に格納された後、移動エージェント５４０は次の移動先である移動先ホストｉ＋１に移動する（ステップＣ２３，２４）。この処理は図６においてステップＣ１６に処理を戻す事に対応する。

【０１２３】

ｋ個の移動先ホスト、移動先ホスト１～移動先ホストｋを訪問した移動エージェント５４０が移動先ホスト１（５１０）に再び戻ってきた後、移動先ホスト１（５１０）は公開鍵暗号計算部５１４を用いて、移動エージェント５４０の中間データ格納５４１に格納されているｅ１ を用いて暗号化されているデータの復号および検証可能である全ての署名の検証を行う（ステップＣ２６）。

【０１２４】

復号および署名検証が済んだ後、移動先ホスト１はG_{k-11}，G_{k-12}，……G_{k-1k}というｋ個のG_{k-1j}（$1 \leqq j \geqq k$）なるデータを保有している。ステップＣ２０での操作と同様

【０１２５】

【数１０】

$$G_{k-1j} = G_{k-1}^{V_{k-1j}} \pmod{p}$$

【０１２６】

という関係とv_{k-1j}が（ｋ，ｎ）閾値秘密分散共有法の部分情報である事に注意すると、

【０１２７】

【数１１】

$$\prod_{j=1}^{k} G_{k-1j}^{L_j} = G_{k-1}^{\sum_{j=1}^{k} L_j v_{k-1j}} = G_{k-1}^{x_{k-1}} \pmod{p}$$

【０１２８】

が成立するので、ＥｌＧａｍａｌ暗号の復号法と比較すると、

【０１２９】

【数１２】

$$r_{k-1} = \frac{M_{k-1}}{\prod_{j=1}^{k} G_{k-1j}^{L_j}} = \frac{M_{k-1}}{G_{k-1}^{x_{k-1}}} \pmod{p}$$

【０１３０】

が成立するので、部分署名計算部にG_{k-11}，G_{k-12}，…，G_{k-1j}を入力する事によって、r_{k-1}が得られる。さらに部分署名部はｍを入力として得る事により部分署名

【０１３１】

【数１３】

$$S_{k-1} = m^{r_{k-1}} \pmod{n}$$

【０１３２】

を出力する（ステップＣ２７）。

ステップＣ２７終了時に移動先ホスト１はｋ個の部分署名Ｓ１，Ｓ２，…，Ｓｋ

を保有している。ここで各Ｓｉが

【０１３３】

【数１４】

$$S_i = m^{r_i} \pmod{n}$$

【０１３４】

という関係を満足する事と、

【０１３５】

【数１５】

$$d_A = \sum_{i=1}^{k-1} r_i \pmod{\mathrm{lcm}(p-1, q-1)}$$

【０１３６】

という関係が成立している事を考慮すると、部分署名署名化部がｋ個の部分署名Ｓｉ（１≦ｉ≦ｋ）を入力とし、

【０１３７】

【数１６】

$$\prod_{i=1}^{k-1} S_i = m^{\sum_{i=1}^{k-1} r_i} = m^{d_A} \pmod{n}$$

【０１３８】

を計算する事によって、移動先ホストが動的に提示した任意のデータｍに対して移動エージェント５４０の所有者の秘密鍵ｄＡ を用いて計算したＲＳＡ署名が得られる。移動先ホスト１（５１０）は上記計算によって得られたデータを移動エージェント５４０によるｍに対する署名として格納する。署名を計算し終えた移動エージェント５４０はベースホスト５００に戻る（ステップＣ２８）。

【０１３９】

次に、第２の実施例を図７および図８を参照して説明する。

本実施例は、前述の第２の実施の形態に係る署名計算方式をＲＳＡ署名方式対応とするものである。

本実施例で用いる情報セキュリティの実現方式であるＲＳＡ署名方式、（ｋ，ｎ）閾値秘密分散共有法、ＥｌＧａｍａｌ暗号方式については上述の第１の実施例と重複するため説明を省略する。

【０１４０】

本実施例では移動エージェントの所有者はＲＳＡ秘密鍵ｄＡ および対応する公開鍵ｅＡ を所有している。また移動先ホストｉ（１≦ｉ≦ｎ）もＲＳＡ秘密鍵ｄｉ および対応する公開鍵ｅｉ を所有している。

【０１４１】

さら本方式全体にはｋ個のＥｌＧａｍａｌ暗号公開鍵ｙｊ（１≦ｊ＜ｋ）が存在し、対応する秘密鍵ｘｊ（１≦ｊ＜ｋ）は（ｊ＋１，ｎ）閾値秘密分散共有法を用いて各移動先ホストｉ（１≦ｉ≦ｎ）に秘密鍵として分散共有されてい

る。以後、移動先ホストｉ（１≦ｉ≦ｎ）が保有する秘密鍵ｘｊ に対する分散情報をｖｉｊと表記する。

【０１４２】

以上の準備の下、図７および図８を参照にして本実施例の処理の流れについて説明する。

まず図７のベースホスト７００において移動エージェント７４０が起動される（図８のステップＤ１）。

【０１４３】

部分署名補助データ生成部７０４は乱数生成部７０１から出力される乱数を入力として新規のＲＳＡの公開鍵（ｒｎ，ｒｅ），秘密鍵ｒｄ および

$$rd = \Sigma ri \pmod{lcm(r_{p-1}, r_{q-1})}$$

を満足する乱数ｒｉ （１≦ｉ＜ｋ）を生成する（ステップＤ２）。ここで、ｒｐ，ｒｑ は素数でありｒｎ ＝ｒｐ ｒｑ を満足する。

【０１４４】

得られた新規公開鍵（ｒｎ，ｒｅ）およびｒｉ に対してはｄＡ による署名が計算され（ステップＤ３）、さらにＥｌＧａｍａｌ暗号公開鍵ｙｉ を用いて暗号文（Ｇｉ，Ｍｉ）が計算された後（ステップＤ４）、新規公開鍵（ｒｎ，ｒｅ），新規公開鍵に対する署名Ｓｐ，暗号文（Ｇｉ，Ｍｉ）およびｒｉ に対する署名は移動エージェント７４０の中間データ格納部７４１に格納される。

【０１４５】

部分署名の計算に必要な補助データを中間データ格納７４１に格納した後、移動エージェント７４０は移動を開始し（ステップＤ５）、いくつかの移動先ホストを動的に巡回した後（ステップＤ６）、ホスト移動中に動的に決定された移動先ホスト１（７１０）に移動し（ステップＤ７，Ｄ８）移動先ホスト１（７１０）が提示したデータｍに対して署名を計算する事を決定する（ステップＤ９）。提示したデータｍに移動エージェント７４０が署名を計算する事を決定した後、移動先ホスト１（７１０）はステップＤ４でベースホストによって計算され中間

データ格納部７４１に格納されている暗号文（Ｇｉ，Ｍｉ）（１≦ｉ＜ｋ）を部分署名計算部７１２に入力する事によってＧｉ１を次式に従って計算する（ステップＤ１０）。

【０１４６】

【数１７】

$$G_{i1} = G_i^{V_{i1}} \pmod{p}$$

【０１４７】

Ｇｉ１（１≦ｉ＜ｋ）を計算した後、さらに移動先ホスト１（７１０）は公開鍵暗号計算部７１４に、Ｇｉ１と移動先ホスト１の秘密鍵ｄ（７１５）を入力する事により、ステップＤ１０で計算したＧｉ１に対する移動先ホスト１のＲＳＡディジタル署名を計算する（ステップＤ１１）。署名計算後、移動先ホスト１はG_{k-11}を移動先ホスト１（７１０）のデータ記憶部７１６に格納し（ステップＤ１２）、残りの計算結果Ｇｉ１（１≦ｉ＜ｋ－１）を中間データ格納部７４１に格納する（ステップＤ１３）。中間データ格納部７４１にへデータ格納をした後、移動エージェント７４０は次の移動先ホストである移動先ホスト２（７２０）に移動する（ステップＤ１４，Ｄ１５）。

【０１４８】

移動エージェント７４０が移動先ホストｉ（２≦ｉ≦ｋ）に移動すると、移動先ホストｉはステップＤ４でベースホスト７００によって計算され中間データ格納部７４１に格納されている暗号文（Ｇｊ，Ｍｊ）（ｉ－１≦ｊ＜ｋ）を部分署名計算部７２２に入力する事によってＧｊｉを次式に従って計算する（ステップＤ１６）。

【０１４９】

【数１８】

$$G_{ji} = G_j^{V_{ji}} \pmod{p}$$

【０１５０】

Ｇｊｉ（ｉ－１≦ｊ＜ｋ）を計算した後、移動先ホストｉは、計算したＧｊｉ

と移動先ホストｉの秘密鍵ｄｉ を公開鍵暗号計算部７２４に入力する事によってＧｊｉに対する移動先ホストｉのＲＳＡ署名を計算し（ステップＤ１７）、さらにＧｋ
－１ｊを署名対象データの提示を行った移動先ホスト１（７１０）の公開鍵ｅ１で暗号化する（ステップＤ１８）。ここで現在移動エージェント７４０が訪問している移動先ホストが移動先ホストｋ（移動先ホスト１（７１０）を訪問後ｋ番目に訪問したホスト）であった場合には、移動エージェントは移動先ホスト１（７１０）に戻る（ステップＤ１９，２５）。

【０１５１】

現在の移動先ホストが移動先ホストｋでない場合、この時点において、移動先ホストｉはG_{i-11}, G_{i-12}, …, G_{i-1i}というｉ個のG_{i-1j}（$1 \leqq j \leqq i$）なるデータを保有している。

【０１５２】

【数１９】

$$G_{i-1j} = G_{i-1}^{V_{i-1j}} \pmod{p}$$

【０１５３】

という関係とv_{i-1j}が（ｉ，ｎ）閾値秘密分散共有法の部分情報である事に注意すると、

【０１５４】

【数２０】

$$\prod_{j=1}^{i} G_{i-1j}^{L_j} = G_{i-1}^{\sum_{j=1}^{i} L_j v_{i-1j}} = G_{i-1}^{x_{i-1}} \pmod{p}$$

【０１５５】

が成立する。ここでＬｊ は、前記の$v_{i-1j} = f_{i-1}(l_j)$なるｌｊ を用いて次式で定義される。以後のＬｊ についても同様に定義されるものとする。

【０１５６】

【数２１】

$$L_j = \prod_{1 \leqq j \leqq j, m \neq j} \frac{l_m}{l_m - l_j} \pmod q$$

【０１５７】

ＥｌＧａｍａｌ暗号の復号法と比較すると、

【０１５８】

【数２２】

$$r_{i-1} = \frac{M_{i-1}}{\prod_{j=1}^{i} G_{i-1j}^{L_j}} = \frac{M_{i-1}}{G_{i-1}^{x_{i-1}}} \pmod p$$

【０１５９】

が成立するので、部分署名計算部にG_{i-11}，G_{i-12}，…，G_{i-1i}を入力して上記計算を行う事によって、r_{i-1}が得られる。さらに部分署名部はｍを入力として得る事により部分署名

【０１６０】

【数２３】

$$S_{i-1} = m^{r_{i-1}} \pmod n$$

【０１６１】

を出力する（ステップＤ２０）。

S_{i-1}が出力された後、移動先ホストｉはS_{i-1}と移動先ホスト１（７１０）の公開鍵ｅ１とを公開鍵暗号計算部に入力してS_{i-1}を暗号化し、さらにS_{i-1}と移動エージェント７４０の所有者の公開鍵ｄｉを公開鍵暗号計算部に入力しS_{i-1}に対する移動先ホストｉのＲＳＡ署名を計算し、得られた暗号文および署名を中間データ格納部７４１に格納する（ステップＤ２１）。

【０１６２】

さらに以後の訪問先ホストで参照される事のないデータであるG_{i-1j}（１≦ｊ≦ｉ）と移動エージェント７４０の所有者の公開鍵ｅＡ を公開鍵暗号計算部に入力する事によって得られるG_{i-1j}に対するＲＳＡ暗号文を中間データ格納部７４１に格納する（ステップＤ２２）。この暗号文データは、後にベースホスト７００に戻った移動エージェント７４０が行ってきた計算を移動エージェント７４０の所有者が検証するために用いられる。

【０１６３】

移動先ホストｉによって計算されたデータが中間データ格納部７４１に格納された後、移動エージェント７４０は次の移動先である移動先ホストｉ＋１に移動する（ステップＤ２３，２４）。この処理は図８においてステップＤ１６に処理を戻す事に対応する。

【０１６４】

ｋ個の移動先ホスト、移動先ホスト１～移動先ホストｋを訪問した移動エージェント７４０が移動先ホスト１（７１０）に再び戻ってきた後、移動先ホスト１（７１０）は公開鍵暗号計算部７１４を用いて、中間データ格納部７４１に格納されているｅ１ を用いて暗号化されているデータの復号および検証可能である全ての署名の検証を行う（ステップＤ２６）。

【０１６５】

復号および署名検証が済んだ後、移動先ホスト１（７１０）はG_{k-11}，G_{k-12}，…，G_{k-1k}というｋ個のG_{k-1j}（１≦ｊ≦ｋ）なるデータを保有している。ステップＤ２０での操作と同様

【０１６６】

【数２４】

$$G_{k-1j} = G_{k-1}^{V_{k-1j}} \pmod{p}$$

【０１６７】

という関係とv_{k-1j}が（ｋ，ｎ）閾値秘密分散共有法の部分情報である事に注意すると、

【０１６８】

【数２５】

$$\prod_{j=1}^{k} G_{k-1j}^{L_j} = G_{k-1}^{\sum_{j=1}^{k} L_j v_{k-1j}} = G_{k-1}^{x_{k-1}} \pmod{p}$$

【０１６９】

が成立するので、Ｅｌ Ｇａｍａｌ暗号の復号法と比較すると、

【０１７０】

【数２６】

$$r_{k-1} = \frac{M_{k-1}}{\prod_{j=1}^{k} G_{k-1j}^{L_j}} = \frac{M_{k-1}}{G_{k-1}^{x_{k-1}}} \pmod{p}$$

【０１７１】

が成立するので、部分署名計算部にG_{k-11}，G_{k-12}，…，G_{k-1i}を入力する事によって、r_{k-1}が得られる。さらに部分署名部はｍを入力として得る事により部分署名

【０１７２】

【数２７】

$$S_{k-1} = m^{r_{k-1}} \pmod{n}$$

【０１７３】

を出力する（ステップＤ２７）。

ステップＤ２７終了時に移動先ホスト１（７１０）はｋ個の部分署名Ｓ１，Ｓ２，…，Ｓｋ を保有している。ここで各Ｓｉ が

【０１７４】

【数２８】

$$S_i = m^{r_i} \pmod{n}$$

【０１７５】

という関係を満足する事と、

【０１７６】

【数２９】

$$r_d = \sum_{i=1}^{k-1} r_i \pmod{\mathrm{lcm}(r_p-1, r_q-1)}$$

【０１７７】

という関係（ここでｒｐ，ｒｑはｒｎ＝ｒｐ ｒｑ となる素数）が成立している事を考慮すると、部分署名署名化部がｋ個の部分署名Ｓｉ （１≦ｉ≦ｋ）を入力とし、

【０１７８】

【数３０】

$$\prod_{i=1}^{k-1} S_i = m^{\sum_{i=1}^{k-1} r_i} = m^{r_d} \pmod{r_n}$$

【０１７９】

を計算する事によって、移動先ホストが動的に提示した任意のデータｍに対して移動エージェント７４０のベースホスト７００が新規に生成した秘密鍵ｒｄ を用いて計算したＲＳＡ署名Ｓ＝m^{rd}が得られる。

【０１８０】

移動先ホスト１（７１０）は上記計算によって得られたＳと移動エージェントのベースホストによって新規に生成されたＲＳＡ公開鍵（ｒｎ，ｒｅ）と、エージェント所有者の秘密鍵ｄＡ による（ｒｎ，ｒｅ）に対する署名S_pの組（Ｓ，（ｒｎ，ｒｅ），Ｓｐ）を移動エージェント７４０によるｍに対する署名として格納する。署名を計算し終えた移動エージェント７４０はベースホスト７００に戻る（ステップＤ２８）。

【０１８１】

尚、各実施の形態および各実施例における移動エージェント、移動先ホストの

各コンピュータシステムにおいて、各フローチャートで説明した移動エージェントで実行される処理、および移動先ホストで実行される処理はコンピュータシステムにおけるＲＯＭ等のメモリに格納されたプログラムに従って実行されるが、このメモリは本発明によるプログラムを記録した記録媒体を構成するものとなる。

このような記録媒体としては、各種のディスク媒体や半導体記憶装置、磁気記録媒体等を用いることができる。

【０１８２】

次に、前述した特表平１１－５０６２２２公報に開示された技術と本発明とを比較検討する。

前記公報の請求項１～３は、「予め定められたエンティティー」の秘密鍵の情報を「予め定められた複数（定数：ｔ０個）の機関」で分散管理し、分散情報を有する複数の機関が署名対象データに対して計算した部分署名を組み合わせることにより、正しいディジタル署名の計算を行う方式となっている。

【０１８３】

また前記公報の請求項４は、「あるエンティティー（不特定と解釈する事も可能）」の署名を計算する権限を「予め定められた複数（定数：ｔ０個）の機関」に一時的に委託することを目的としており、「あるエンティティー」の秘密鍵の部分情報を予め定められた複数の機関に渡し、分散情報を有する複数の機関が署名対象データに対して計算した部分署名を組み合わせることにより、正しいディジタル署名の計算を行う方式となっている。

【０１８４】

これに対して本発明は、「不特定のエンティティー（本発明では移動エージェントの所有者）」の秘密鍵によるディジタル署名の計算を「不特定（エージェントが事前に知る事ができない）複数（定数）の機関（本発明では移動先ホスト）」に委託することを目的とし、不特定複数のどの移動先ホストが部分署名を計算した場合でも、正しいディジタル署名が計算されるという方式である（移動先ホストが移動エージェントが出発する前に部分署名を計算するホストを知る事ができない事は、前述により説明した通りである）。

【０１８５】

前記公報の請求項４を、その記載されている目的とは異なった使い方をする事によって、「不特定の複数の機関」に署名計算を委託する方式に転用する事は不可能ではないが（例えば署名計算を委託する可能性のある全ての機関からｔ０個を取り出す全ての可能な組み合わせに対して秘密鍵の部分情報を計算する等）、しかし、本発明が意図しているような署名計算を委託する可能性のある機関が膨大な数になるような場合には、効率の面から考えて大きなデメリットがあるものである。

【０１８６】

例えば、移動エージェントが移動のために携えていくデータサイズについて考えると、本発明では、ｔ０個に比例したサイズになるが、前記公報の技術では、署名計算を委託する可能性のあるホスト（個数ｎ）を不特定にしようとした場合には、ｔ０＊ｎＣｔ０に比例したサイズになってしまう（ここでａＣｂは、ａ個の中からｂ個を取り出す可能な組み合わせの個数を表す）。

【０１８７】

以上述べたことから、

（１）本発明の方式は、部分署名の計算を行う機関が不特定である。即ち、前記公報の技術とは意図が異なる。

（２）仮に前記公報の方式を部分署名の計算を行う機関が不特定な場合に適用しようとしても、効率の面から問題があり、このような場合は、本発明を適用する方がメリットが大きいと言える。

【０１８８】

【発明の効果】

本発明の効果は、ｋ個（ｋ：定数）の移動先ホストが結託しない限り移動エージェントの所有者の秘密鍵によるディジタル署名を偽造が困難であるような形で移動エージェントにデータを持たせつつ、移動エージェントは移動先で提示される任意のデータに対して移動エージェントの所有者の秘密鍵を用いたディジタル書名を移動中に計算できることにある。

【０１８９】

その理由は、移動エージェントが署名を計算するためには、ｋ個の移動先ホストによる部分署名が必要であり、部分署名の計算には移動先ホストの秘密鍵の情報が必要であるため、署名の偽造を行おうとした場合には、ｋ個の秘密鍵を用いた演算が必要となるので、ｋ個の移動先ホストが結託しない限りは署名の偽造が困難となるためである。

【図面の簡単な説明】

【図１】　本発明の第１の実施の形態による移動エージェントによる署名計算システムの構成を示すブロック図である。

【図２】　第１の実施の形態の動作を示すフローチャートである。

【図３】　本発明の第２の実施の形態による移動エージェントによる署名計算システムの構成を示すブロック図である。

【図４】　第２の実施の形態の動作を示すフローチャートである。

【図５】　本発明の第１の実施例による移動エージェントによる署名計算システムの構成を示すブロック図である。

【図６】　第１の実施例の動作を示すフローチャートである。

【図７】　本発明の第２の実施例による移動エージェントによる署名計算システムの構成を示すブロック図である。

【図８】　第２の実施例の動作を示すフローチャートである。

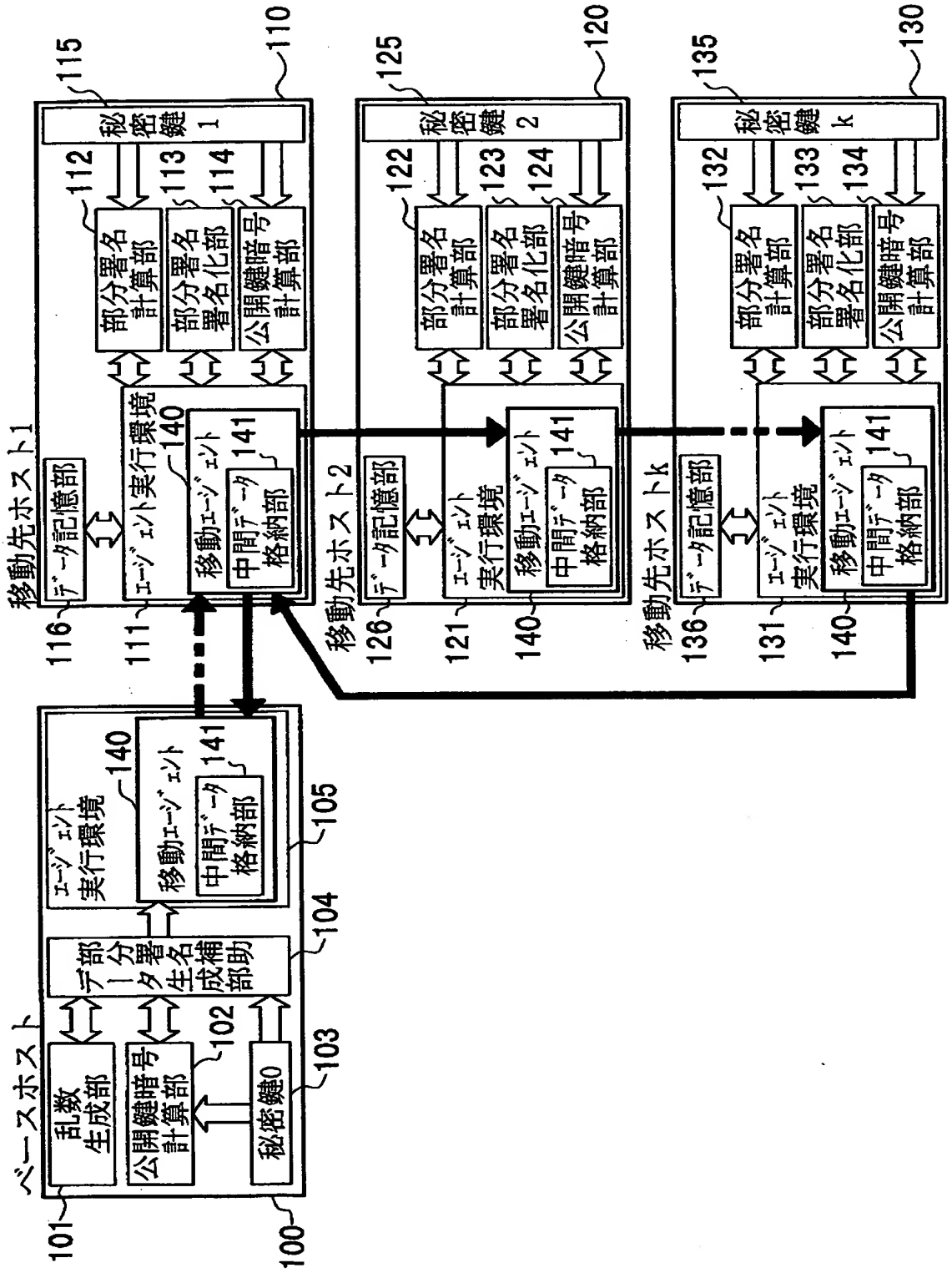
【符号の説明】

１００，３００，５００，７００　ベースホスト
１０１，３０１，５０１，７０１　乱数生成部
１０２，３０２，５０２，７０２　公開鍵暗号計算部
１０３，３０３，５０３，７０３　秘密鍵
１０４，３０４，５０４，７０４　部分署名補助データ生成部
１０５，３０５，５０５，７０５　エージェント実行環境
１１０，３１０，５１０，７１０　移動先ホスト１
１２０，３２０，５２０，７２０　移動先ホスト２
１３０，３３０，５３０，７３０　移動先ホストｋ
１１１，１２１，１３１，

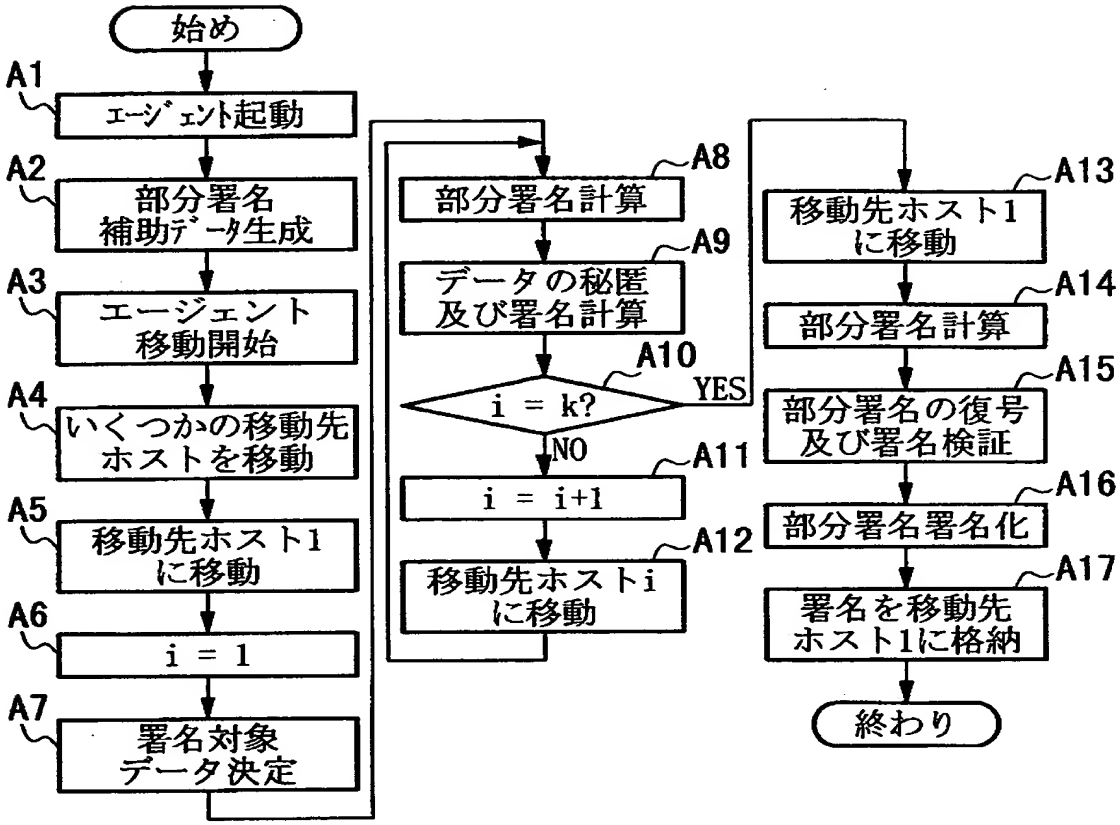
３１１，３２１，３３１，
５１１，５２１，５３１，
７１１，７２１，７３１　　エージェント実行環境
１１２，１２２，１３２，
３１２，３２２，３３２，
５１２，５２２，５３２，
７１２，７２２，７３２　　部分署名計算部
１１３，１２３，１３３，
３１３，３２３，３３３，
５１３，５２３，５３３，
７１３，７２３，７３３　　部分署名署名化部
１１４，１２４，１３４，
３１４，３２４，３３４，
５１４，５２４，５３４，
７１４，７２４，７３４　　公開鍵暗号計算部
１１５，１２５，１３５，
３１５，３２５，３３５，
５１５，５２５，５３５，
７１５，７２５，７３５　　秘密鍵
１１６，１２６，１３６，
３１６，３２６，３３６，
５１６，５２６，５３６，
７１６，７２６，７３６　　データ記憶部
１４０，３４０，５４０，７４０　移動エージェント
１４１，３４１，５４１，７４１　中間データ格納部

【書類名】　　図面

【図１】

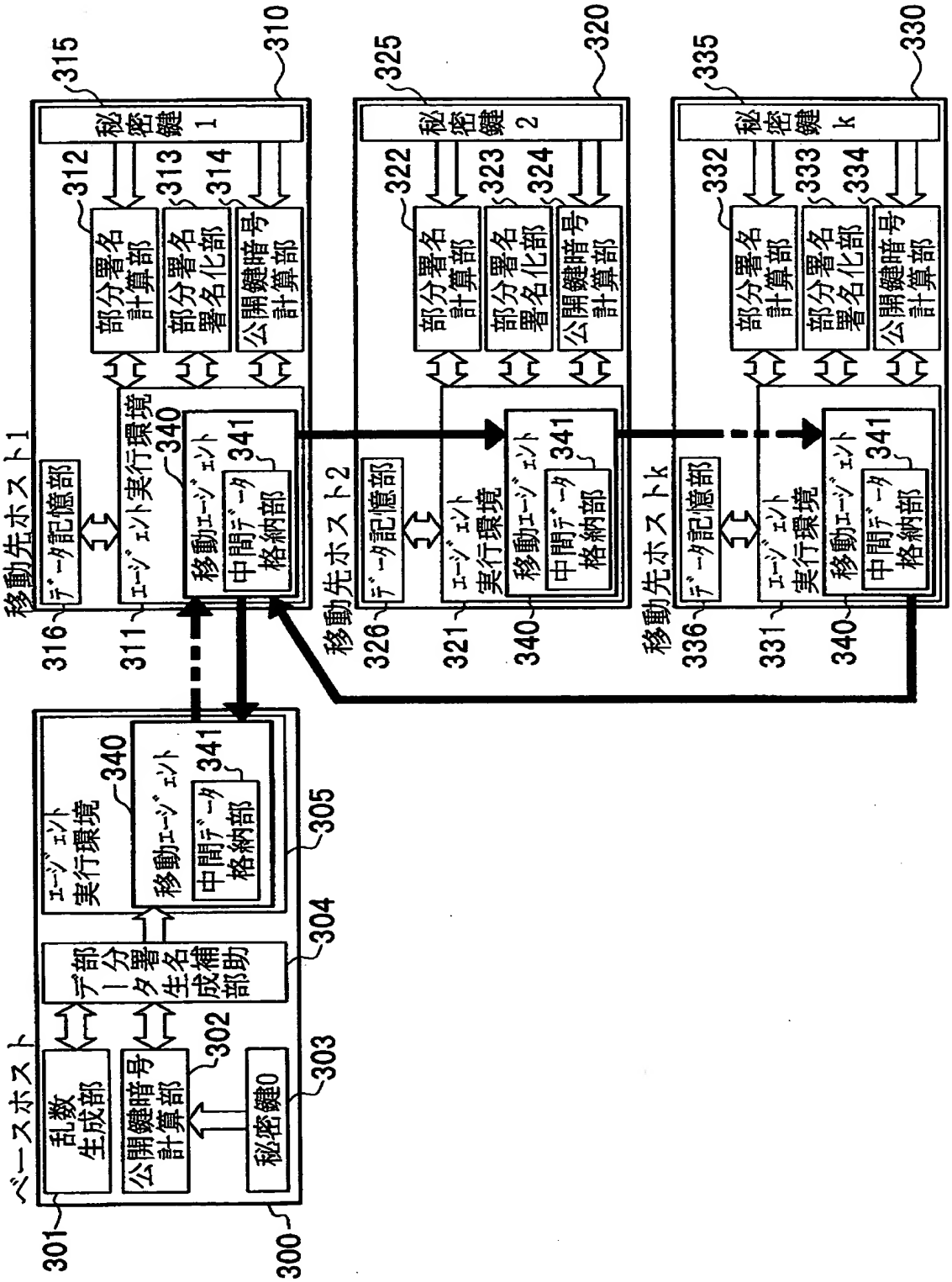

ベースホスト
乱数生成部
公開鍵暗号計算部
データ部分署名生成補助
秘密鍵0
エージェント実行環境
移動エージェント
中間データ格納部
移動先ホスト1
データ記憶部
エージェント実行環境
移動エージェント
中間データ格納部
部分署名計算部
部分署名化部
公開鍵暗号計算部
秘密鍵1
移動先ホスト2
秘密鍵2
移動先ホストk
秘密鍵k
100
101
102
103
104
105
110
111
112
113
114
115
116
120
121
122
123
124
125
126
130
131
132
133
134
135
136
140
141

【図２】

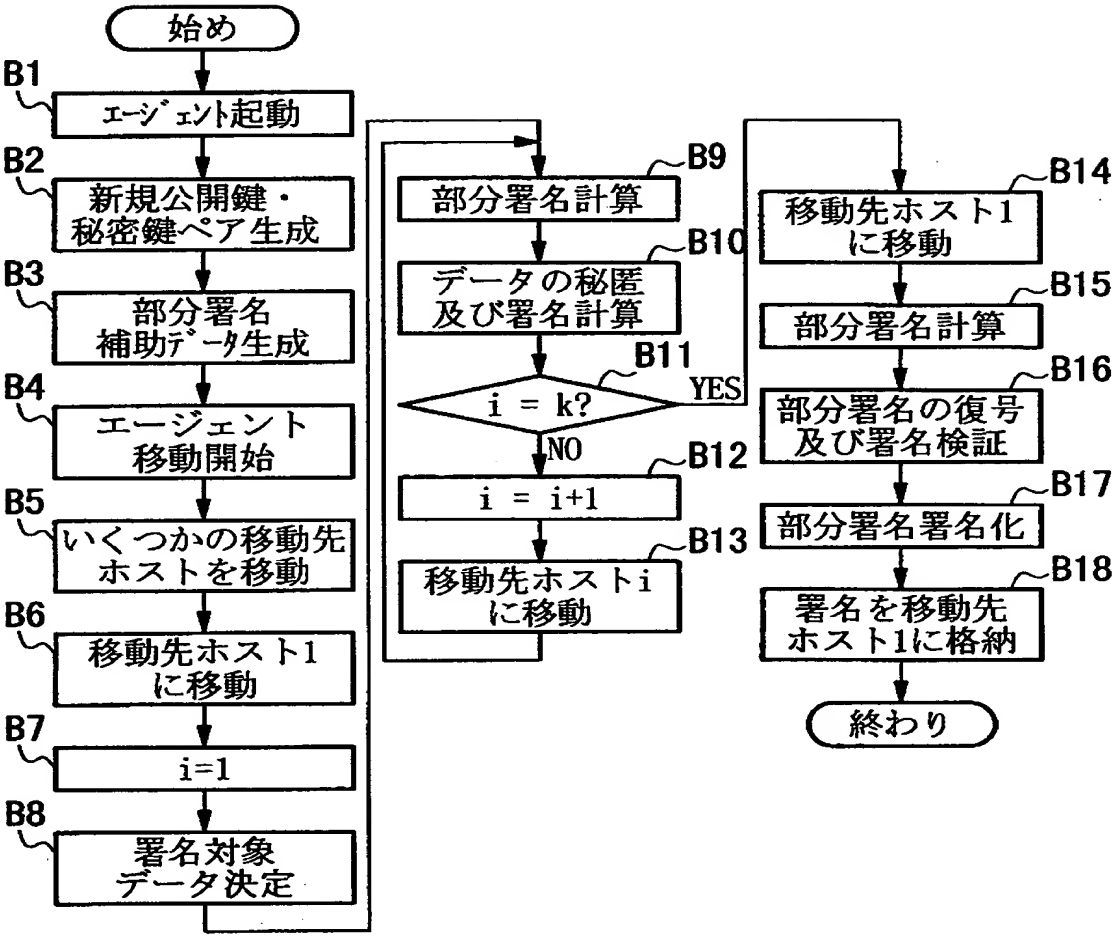


出証特２０００－３０８４３８３

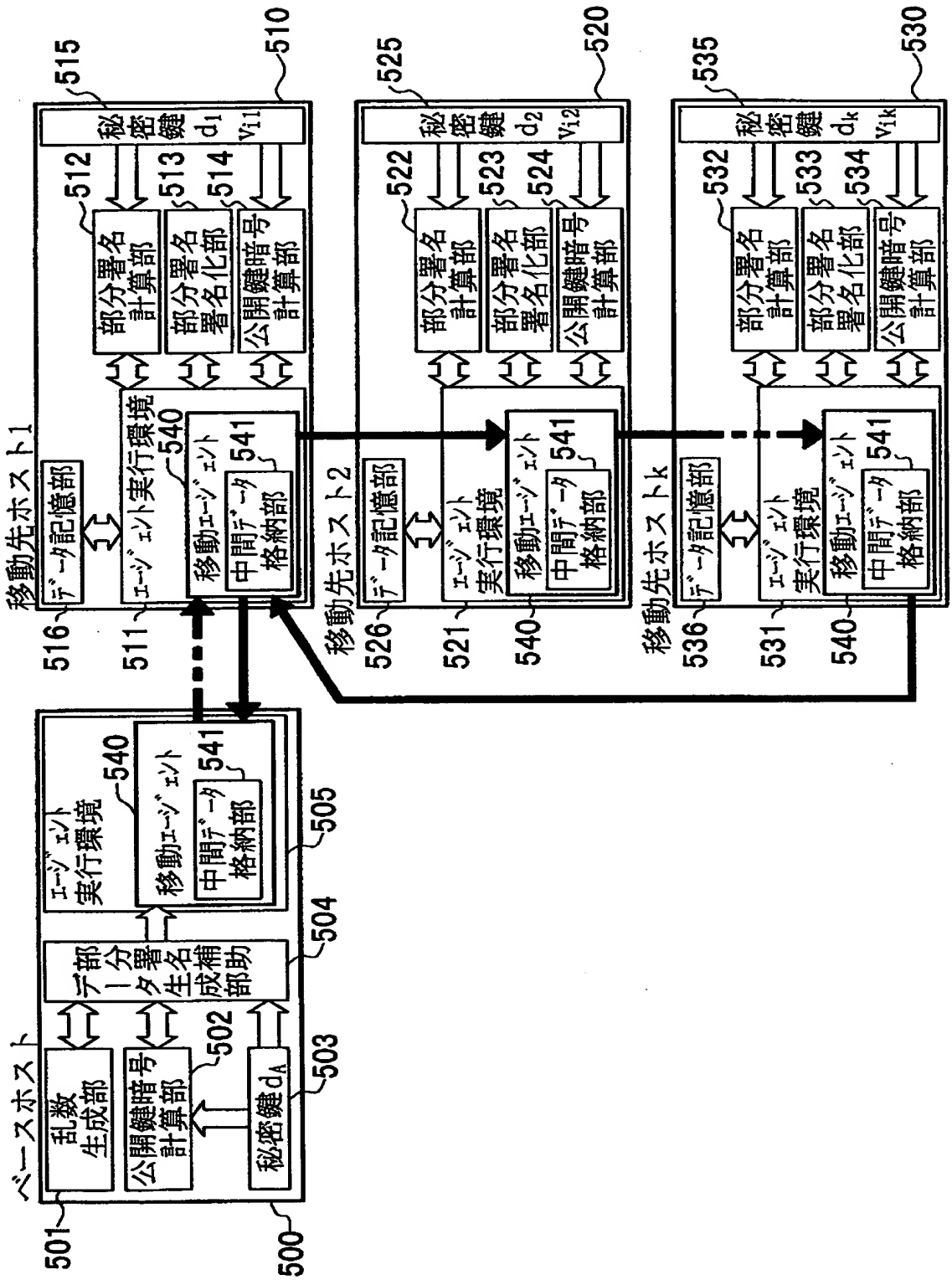
【図３】


ベースホスト
乱数生成部
公開鍵暗号計算部
秘密鍵0
部分署名生成補助
エージェント実行環境
移動エージェント
中間データ格納部
301
302
303
304
305
300
移動先ホスト1
データ記憶部
エージェント実行環境
移動エージェント
中間データ格納部
秘密鍵1
部分署名計算部
部分署名化部
公開鍵暗号計算部
316
311
340
341
315
312
313
314
310
移動先ホスト2
データ記憶部
エージェント実行環境
移動エージェント
中間データ格納部
秘密鍵2
部分署名計算部
部分署名化部
公開鍵暗号計算部
326
321
340
341
325
322
323
324
320
移動先ホストk
データ記憶部
エージェント実行環境
移動エージェント
中間データ格納部
秘密鍵k
部分署名計算部
部分署名化部
公開鍵暗号計算部
336
331
340
341
335
332
333
334
330

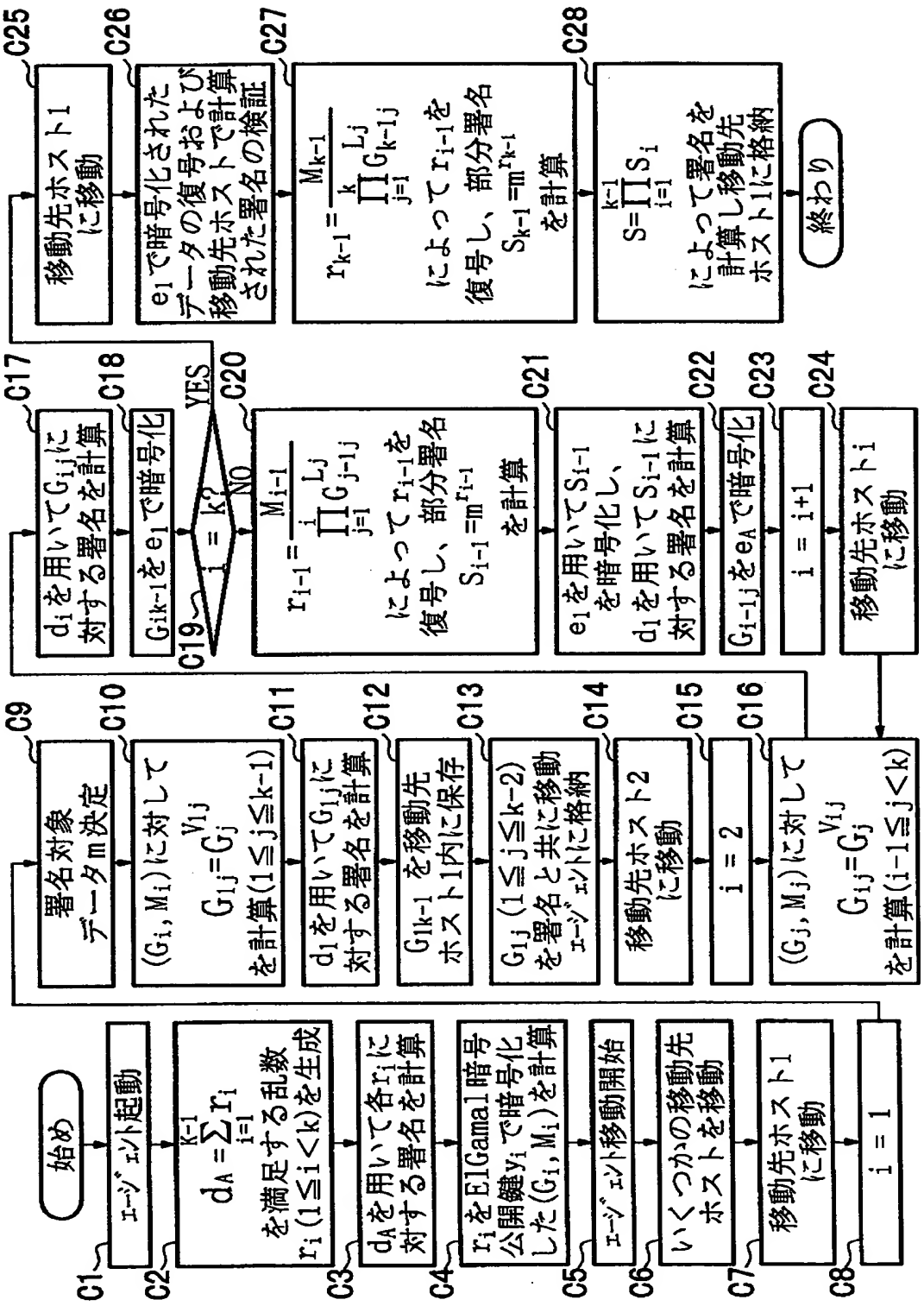
【図４】


始め
B1
エージェント起動
B2
新規公開鍵・
秘密鍵ペア生成
B3
部分署名
補助データ生成
B4
エージェント
移動開始
B5
いくつかの移動先
ホストを移動
B6
移動先ホスト1
に移動
B7
i=1
B8
署名対象
データ決定
B9
部分署名計算
B10
データの秘匿
及び署名計算
B11
i = k?
YES
NO
B12
i = i+1
B13
移動先ホストi
に移動
B14
移動先ホスト1
に移動
B15
部分署名計算
B16
部分署名の復号
及び署名検証
B17
部分署名署名化
B18
署名を移動先
ホスト1に格納
終わり

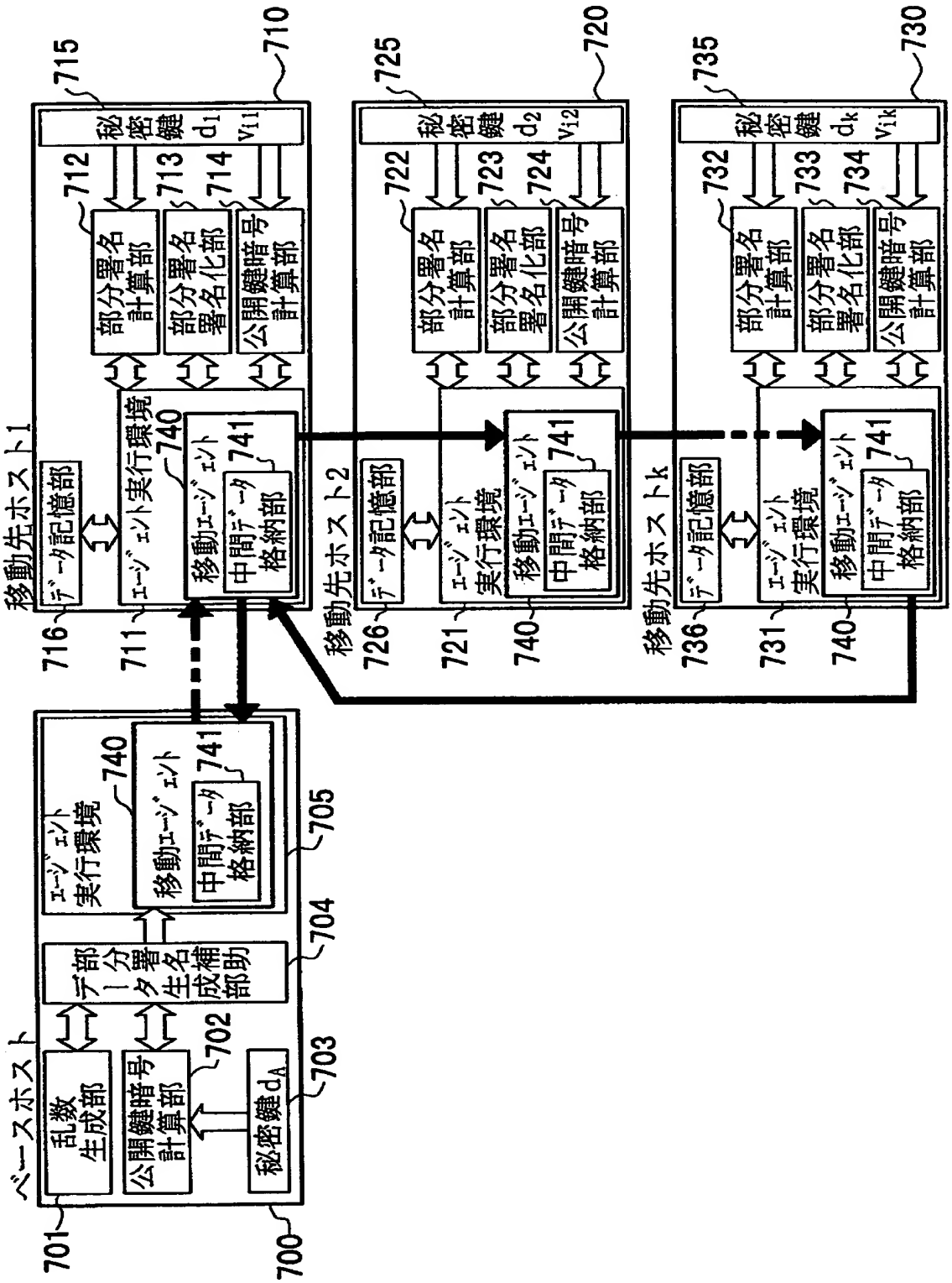
【図５】


ベースホスト
乱数生成部
公開鍵暗号計算部
秘密鍵 d_A
部分署名生成補助部
エージェント実行環境
移動エージェント
中間データ格納部
501
502
503
504
505
500
移動先ホスト1
データ記憶部
エージェント実行環境
移動エージェント
中間データ格納部
部分署名計算部
部分署名署名化部
公開鍵暗号計算部
秘密鍵 d_1 v_{i1}
510
511
512
513
514
515
516
移動先ホスト2
d_2 v_{i2}
520
521
522
523
524
525
526
移動先ホストk
d_k v_{ik}
530
531
532
533
534
535
536
540
541

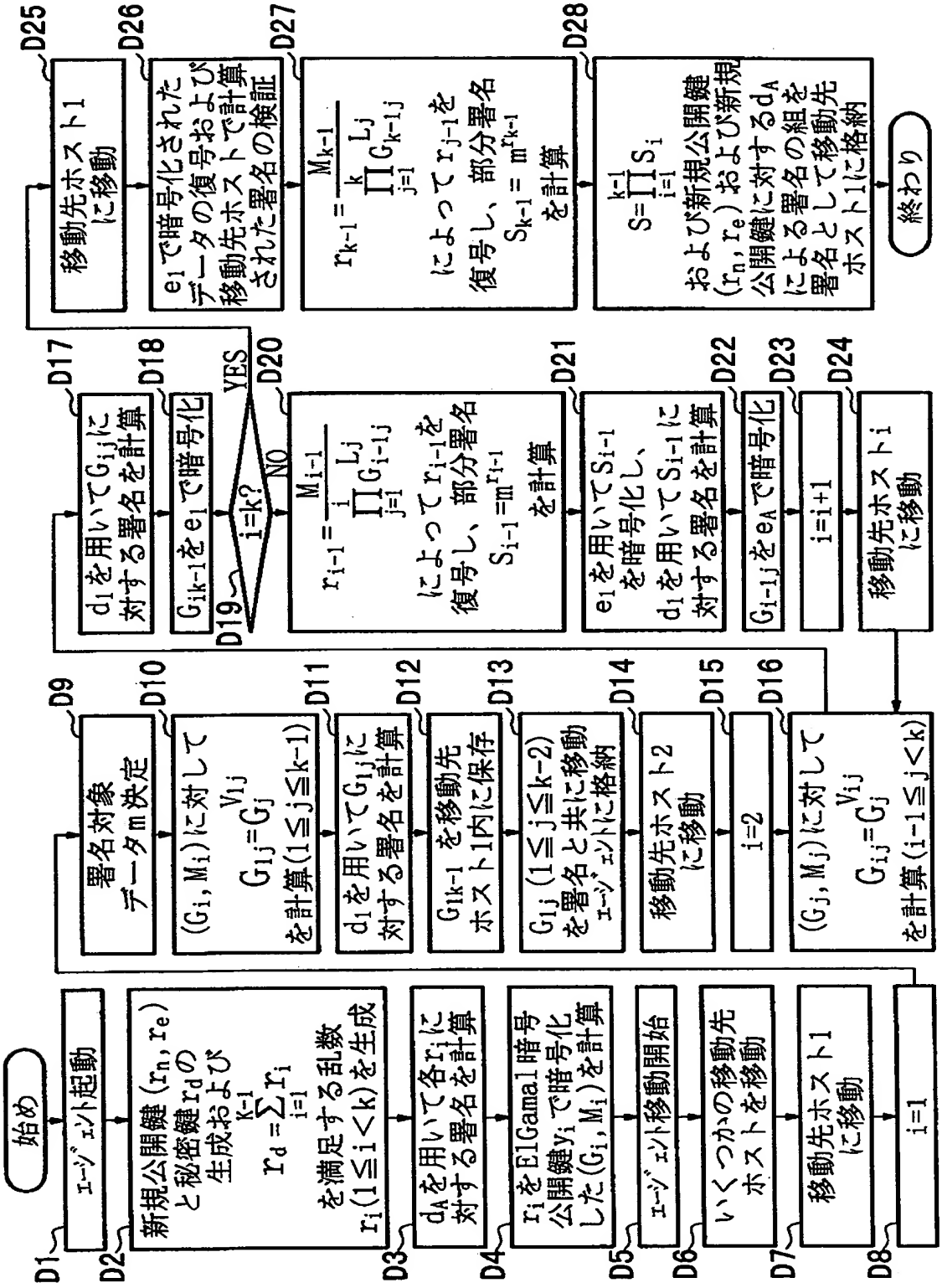
【図６】


始め
C1 エージェント起動
C2 $d_A=\sum_{i=1}^{k-1} r_i$ を満足する乱数 r_i $(1\leqq i<k)$ を生成
C3 d_A を用いて各 r_i に対する署名を計算
C4 r_i をE1Gamal暗号公開鍵 y_i で暗号化した (G_i, M_i) を計算
C5 エージェント移動開始
C6 いくつかの移動先ホストを移動
C7 移動先ホスト1に移動
C8 i = 1
C9 署名対象データmを決定
C10 (G_i, M_i) に対して $G_{1j}=G_j^{V_{1j}}$ を計算$(1\leqq j\leqq k-1)$
C11 d_1 を用いて G_{1j} に対する署名を計算
C12 G_{1k-1} を移動先ホスト1内に保存
C13 G_{1j} $(1\leqq j\leqq k-2)$ を署名と共にエージェントに格納
C14 移動先ホスト2に移動
C15 i = 2
C16 (G_j, M_j) に対して $G_{ij}=G_j^{V_{ij}}$ を計算$(i-1\leqq j<k)$
C17 d_i を用いて G_{ij} に対する署名を計算
C18 G_{ik-1} を e_1 で暗号化
C19 i = k?
YES
NO
C20 $r_{i-1}=\frac{M_{i-1}}{\prod_{j=1}^{i} G_{j-1j}^{L_j}}$ によって r_{i-1} を復号し、部分署名 $S_{i-1}=m^{r_{i-1}}$ を計算
C21 e_1 を用いて S_{i-1} を暗号化し、d_1 を用いて S_{i-1} に対する署名を計算
C22 G_{i-1j} を e_A で暗号化
C23 i = i+1
C24 移動先ホスト i に移動
C25 移動先ホスト1に移動
C26 e_1 で暗号化されたデータの復号および移動先ホストで計算された署名の検証
C27 $r_{k-1}=\frac{M_{k-1}}{\prod_{j=1}^{k} G_{k-1j}^{L_j}}$ によって r_{i-1} を復号し、部分署名 $S_{k-1}=m^{r_{k-1}}$ を計算
C28 $S=\prod_{i=1}^{k-1} S_i$ によって署名を計算し移動先ホスト1に格納
終わり

【図７】


ベースホスト
乱数生成部
公開鍵暗号計算部
秘密鍵 d_A
データ部分署名生成補助部
エージェント実行環境
移動エージェント
中間データ格納部
移動先ホスト1
データ記憶部
エージェント実行環境
移動エージェント
中間データ格納部
秘密鍵 d_1 v_{i1}
部分署名計算部
部分署名署名化部
公開鍵暗号計算部
移動先ホスト2
秘密鍵 d_2 v_{i2}
移動先ホストk
秘密鍵 d_k v_{ik}
700
701
702
703
704
705
710
711
712
713
714
715
716
720
721
722
723
724
725
726
730
731
732
733
734
735
736
740
741

【図８】


始め
D1
エージェント起動
D2
新規公開鍵(rn, re)と秘密鍵rdの生成および
$r_d = \sum_{i=1}^{K-1} r_i$
を満足する乱数ri(1≦i<k)を生成
D3
dAを用いて各riに対する署名を計算
D4
riをElGamal暗号公開鍵yiで暗号化した(Gi, Mi)を計算
D5
エージェント移動開始
D6
いくつかの移動先ホストを移動
D7
移動先ホスト1に移動
D8
i=1
D9
署名対象データm決定
D10
(Gi, Mi)に対して
$G_{1j}=G_j^{V_{1j}}$
を計算(1≦j≦k-1)
D11
d1を用いてG1jに対する署名を計算
D12
G1k-1を移動先ホスト1内に保存
D13
G1j (1≦j≦k-2)を署名と共に移動エージェントに格納
D14
移動先ホスト2に移動
D15
i=2
D16
(Gj, Mj)に対して
$G_{ij}=G_j^{V_{ij}}$
を計算(i-1≦j<k)
D17
d1を用いてGijに対する署名を計算
D18
Gik-1をe1で暗号化
D19
i=k?
YES
NO
D20
$r_{i-1}=\frac{M_{i-1}}{\prod_{j=1}^{i} G_{i-1j}^{L_j}}$
によってri-1を復号し、部分署名
$S_{i-1}=m^{r_{i-1}}$
を計算
D21
e1を用いてSi-1を暗号化し、d1を用いてSi-1に対する署名を計算
D22
Gi-1jをeAで暗号化
D23
i=i+1
D24
移動先ホストiに移動
D25
移動先ホスト1に移動
D26
e1で暗号化されたデータの復号および移動先ホストで計算された署名の検証
D27
$r_{k-1}=\frac{M_{k-1}}{\prod_{j=1}^{k} G_{k-1j}^{L_j}}$
によってrj-1を復号し、部分署名
$S_{k-1}=m^{r_{k-1}}$
を計算
D28
$S=\prod_{i=1}^{k-1} S_i$
および新規公開鍵(rn, re)および新規公開鍵に対するdAによる署名の組を署名として移動先ホスト1に格納
終わり

【書類名】　　要約書

【要約】

【課題】　プログラム・コードおよびデータを解析されても、移動先のホストに署名を偽造されない形で移動エージェントにデータを保持させ、移動先のホストで提示された任意のデータに対してディジタル署名を計算させるようにする。

【解決手段】　移動エージェント１４０が起動されるベースホスト１００において、移動エージェントの所有者の秘密鍵０（１０３）を、部分署名補助データ生成部１０４によってｋ個の移動先ホスト１１０、１２０、１３０の秘密鍵１１５、１２５、１３５を用いた演算を行うことではじめて復元可能となるような形態に分割する。移動エージェントが訪れる各移動先ホストは、移動エージェントに格納されたデータと移動先ホストの秘密鍵とを部分署名計算部１１２，１２２，１３２への入力として部分署名を計算し、ｋ個のホストが計算した部分署名から部分署名署名化部１１３，１２３，１３３を用いて実際の署名を得る。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－００９０３７
受付番号	５００００４４６２４
書類名	特許願
担当官	高田　良彦　　２３１９
作成日	平成１２年　１月２４日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 000004237
- 【住所又は居所】 東京都港区芝五丁目７番１号
- 【氏名又は名称】 日本電気株式会社

【代理人】 申請人
- 【識別番号】 100108578
- 【住所又は居所】 東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
- 【氏名又は名称】 高橋　詔男

【代理人】
- 【識別番号】 100064908
- 【住所又は居所】 東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
- 【氏名又は名称】 志賀　正武

【選任した代理人】
- 【識別番号】 100101465
- 【住所又は居所】 東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
- 【氏名又は名称】 青山　正和

【選任した代理人】
- 【識別番号】 100108453
- 【住所又は居所】 東京都新宿区高田馬場３丁目２３番３号　ＯＲビル　志賀国際特許事務所
- 【氏名又は名称】 村山　靖彦

次頁無

出証特２０００－３０８４３８３

出　願　人　履　歴　情　報

識別番号　　〔０００００４２３７〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社